City of Redondo Beach

CityLaw Master Services Agreement

Prepared for City Attorney's Office
by Cycom —
accounts@cycominc.com

Dear Jennifer & team,

You do important work, and we want to help you do it.

Managing risk and caseload for a City is daunting and complex. CityLaw captures and tracks all your data to keep you aware of risks and workload status.

We always enjoy seeing how much our solutions benefit our customers. We look forward to working with your team to launch CityLaw for the City of Redondo Beach.

Best,

Bobby W. Jones II
President. Cycom Data Systems

About this Agreement

This page allows you to build a subscription that suits your needs.

You can scroll down to move through each section of this page sequentially or use the menu button at the top- right to jump between sections.

City Investment

Use the "City Investment" section to select your subscription tier, number of users, and add-ons.

ROI Calculator

Use the ROI calculator to see how much you can save with CityLaw.

Agreement Sections

You can review all the terms and conditions in Agreement sections:

1. Master Services Agreement (MSA)
2. Statement of Work (SOW)
3. Exhibit A-2-a (CityLaw Rider)
4. Exhibit A-9 (Support and Maintenance Rider)

Accept & Sign

When you're finished building your subscription and reviewing this Agreement, e-sign in this section and we will set up your CityLaw system and reach out to you to schedule your CityLaw training sessions!

We can't wait to show you how CityLaw can save your team time and money and help you serve your community even better.

Important Contacts

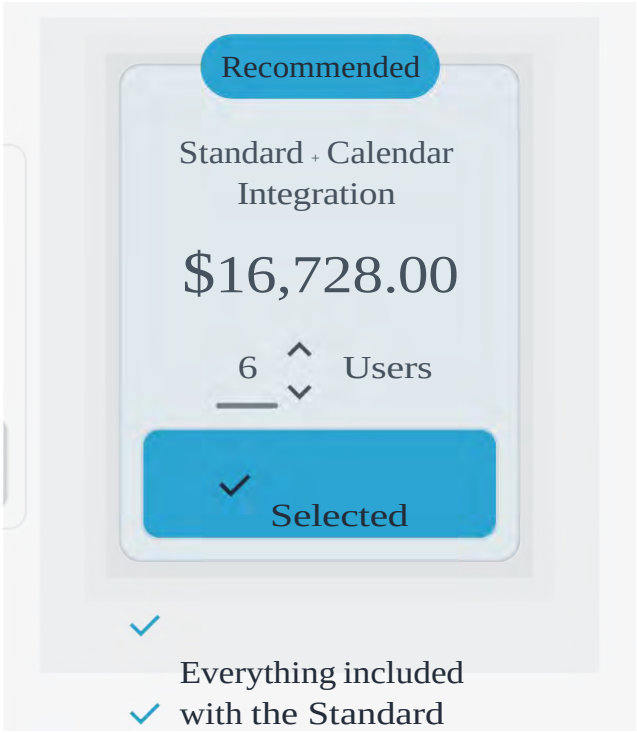
While filling out the Acceptance Form on this page, you will need to provide the contact information of the personnel who should be assigned to the important roles on your account:

1. Account Holder: Authorized to handle all matters related to billing.
2. System Administrators (1 & 2): Know the System's administrator password, can manage System security profiles for users, and are authorized to receive the Password of the Day (POTD) which enables them to deny or grant file access to specific users, overriding the System security profiles of the user(s). System Administrators are also authorized to grant approval for and schedule system upgrades or maintenance.
3. IT Contact: Has full control over the computing resources which host the System. They will assist with System upgrades and maintenance or will be responsible for delegating such work to appropriate IT personnel.

City INVESTMENT

Note: As requested, this is a draft quote for STAGE ONE. The final proposal price may vary if needs / conditions change.

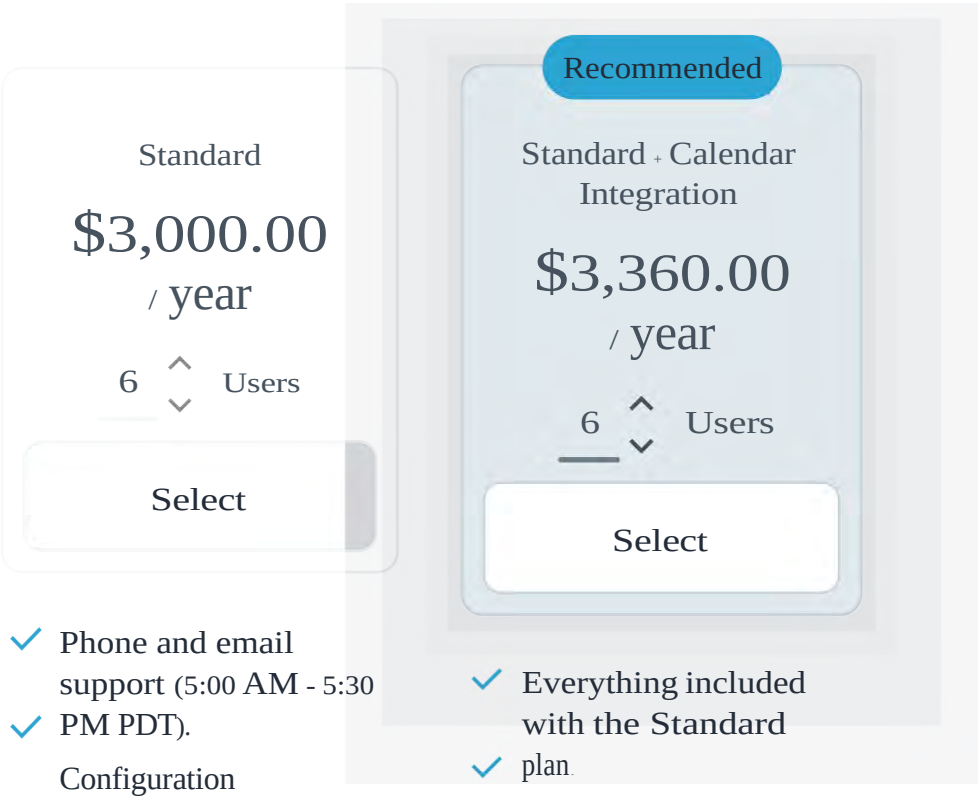
Licensing



- 8 hours of customized remote training.
- End-to-end implementation assistance.
- Document template automation.
- Custom Reporting assistance.
- Dashboard configuration.
- Microsoft Word and Excel integration.

- Everything included with the Standard Licensing
- Microsoft Outlook Calendar integration.

Support and Maintenance



- Phone and email support (5:00 AM - 5:30 PM PDT).
- Configuration consultation.
- Data integrity reviews.
- Free upgrades to new features, security improvements, and bug fixes for CityLaw.

- Everything included with the Standard plan.
- Phone and email support (5:00 AM - 5:30 PM) for Calendar Integration.
- Free upgrades to new Calendar Integration features, security improvements, and bug fixes.

Web Portals

SUBTOTAL
$3,000.00

Description	Item	Quantity	Price
☑ Work Assignment Portal	$3,000.00	1 Portal	$3,000.00
☐ Discrimination Complaint Portal	$6,000.00	1 Portal	$6,000.00
☐ Claim Intake Portal	$3,000.00	1 Portal	$3,000.00

Conversion of Existing Data

SUBTOTAL
$0.00

Description	Item	Quantity	Price
☐ Data Conversion Services	$125.00	20 Hour	$2,500.00

Total Discount	$0.00
Total Excluding Tax	$19,728.00
Total	$19,728.00

ESTIMATED SAVINGS

Master Services Agreement

This Master Services Agreement ("MSA") is entered into, to be effective as of October 1, 2024 (the "Effective Date"), by and between Cycom Data Systems, Inc., a California corporation having a mailing address at P.O. Box 802, Richmond, KY 40476-0802 ("Cycom") and the City of Redondo Beach, a municipal corporation having a principal office address at 415 Diamond Street, Redondo Beach, CA 90277 (the "Municipality"). Either of Cycom and the Municipality may be referred to herein as a "Party," and together as the "Parties."

Recitals

Whereas, Cycom is a provider of certain Services (as defined below), and desires to provide such Services to the Municipality.

Whereas, the Municipality desires to engage Cycom to provide such Services to the

Municipality. Now, therefore, the Parties agree as follows:

1. The Services

During the Term, and subject to the terms and conditions of this MSA, Cycom shall provide to the Municipality certain services, including activities and software and other deliverables (collectively, the "Services"). The particular Services provided to the Municipality by Cycom shall be as specifically set forth in the Statement of Work ("SOW") attached hereto as Exhibit A, or in any other SOW containing substantially similar information. Each such SOW shall be incorporated into and made a part of and governed by the terms of this MSA. Unless expressly provided for in this MSA or in an SOW, in the event of a conflict between the provisions contained in this MSA and those contained in such SOW, the provisions contained in this MSA shall prevail.

2. Certain Defined Terms

As used in this Agreement, each capitalized term that is parenthetically or otherwise defined in any other
section of this Agreement, or in the introductory paragraph of this Agreement, shall have the meaning so ascribed to it, and each of the following terms shall have the meaning ascribed to it in this section.

1. "Access Credentials" means any user name, account name, identification number, password, license or security key, security token, PIN, or other security code, method, technology, or device used, alone or in combination, to verify an individual's identity and authorization to access and use the
Services.

2. "Account Holder" means the authorized agent of the Municipality who is authorized to handle, and is responsible for handling, all matters related to billing that may arise pursuant to the terms and conditions of this MSA.

3. "Documentation" means any manuals, instructions, training materials, or other documents or materials that Cycom provides or makes available to the Municipality in any form or medium and which describe the functionality, components, features, or requirements of the Services, including any aspect of the installation, configuration, integration, operation, use, support, or maintenance of the Software or other components of the Services.

4. "Password of the Day" means a password which is changed daily by Cycom, and which is provided by Cycom to the System Administrator upon request, enabling the System Administrator to deny or grant file access to specific Users and to override the System security profiles of such Users.

5. "Primary IT Contact" means the authorized agent of the Municipality who is: (A) authorized to control, and has responsibility for controlling, all aspects of the Municipality's access to and use of
the System; (B) authorized to assist with, and has responsibility for assisting with, system upgrades
and maintenance with respect to the System; and (C) authorized to delegate any of the responsibilities of the Primary IT Contact to appropriate IT personnel.

6. "Software" means all versions and releases of and updates to the executable, object code version of the proprietary CityLaw/CountyLaw legal case management software developed and owned by Cycom, together with all utilities, add-ins, plug-ins, modules, applets, and the like developed and owned by Cycom and designed to work in conjunction with the CityLaw/CountyLaw software, and including all features and components that allow the CityLaw/CountyLaw software to interface
with other software developed and owned by third parties. In addition to legal case management functions, the Software may also include, without limitation, time management, contract management, claims processing, document management, payment processing, billing, and

other similar or related functions and features.

7. "System" means the computing resources, including software, hardware, networks, and databases and database management systems, that host the Software and database management systems, that host the Software.

8. "System Administrator" means the authorized agent of the Municipality who is: (A) authorized to have, and has responsibility for, access to the administrator password of the System; (B) authorized to manage, and has responsibility for managing, System security profiles for Users; (C) authorized to receive, and has responsibility for receiving, the Password of the Day; and (D) authorized to grant approval for and schedule, and has responsibility for granting approval for and scheduling, System upgrades and maintenance.

9. "Users" means personnel of the Municipality who are authorized and licensed to access the System and use the Software, pursuant to the terms and conditions of this MSA, and for whom access to and use of the System and the Software has been purchased hereunder.

3. Contact Persons

Cycom shall designate a contact person, as described in the applicable SOW, who shall be responsible for communication with the Municipality with respect to the Services and matters related thereto. The Municipality shall designate an Account Holder, a Primary IT Contact, and one (1) or more System Administrators, as described in the applicable SOW, each of whom shall be responsible for communication with Cycom with respect to any matter related to the Services that falls within his or her areas of responsibility. If the Municipality wishes to replace any of the Account Holder, Primary IT Contact or System Administrators, it shall promptly provide written notice to Cycom of such replacement.

4. Software Licensing — In General

1. Incorporation of License Agreements. The software and all software upgrades and version releases and other enhancements, modifications or fixes to the software provided to the Municipality pursuant to this MSA constitute software licensed or sublicensed to the Municipality under any applicable license agreement between (i) the Municipality, and (ii) either Cycom or the third-party vendor of such software (each a "License Agreement"). This MSA is not an amendment to any such License Agreement but is a separate binding agreement that incorporates the terms of any such License Agreement including, without limitation, terms relating to license and ownership rights, use limitations, limitation of liability, and confidentiality and non-disclosure obligations. Cycom uses and has used any and all software and other materials distributed under a free, open source, or similar licensing model ("Open Source Software") in material compliance with all license terms applicable to such Open Source Software; and Cycom has not used or distributed and does not use or distribute any Open Source Software in any manner that requires or has required: (A) Cycom to permit reverse engineering of any software code or other technology owned by Cycom, or (B) any software code or other technology owned by Cycom to be (1) disclosed or distributed in source code form, (2) licensed for the purpose of making derivative works or (3) redistributed at no charge.

2. Unlicensed Software. Cycom does not provide support for the installation or use of unlicensed software. The Municipality shall ensure that it has a licensed copy of all software to which the Services shall apply.

3. Third Party Software Vendors. With respect to third-party software provided to the Municipality pursuant to this MSA: (i) the Municipality explicitly grants to Cycom the right to share the Municipality's license or sublicense information, including all license-related keys and numbers, payroll keys and numbers, and number of users subscribed with Cycom, with the applicable third- party software vendor for verification and tracking purposes; and (ii) the applicable third-party software vendor is responsible solely for the corresponding third-party software itself, and not for the Services, nor any other product or service offered by Cycom directly or through third parties.

4. New Cycom Products. The Municipality understands and agrees that Cycom may develop and market new or different products and services which may incorporate part or all of the Software and the Documentation and which may perform part or all of the functions performed by the Services. Except as expressly stipulated in this MSA, nothing shall give the Municipality any rights to such new or different products and services.

5. Software as a Service (SaaS)

SaaS Authorization of Access and Use. Subject to and conditioned on the Municipality's and its authorized Users' compliance with the terms and conditions of this MSA, Cycom hereby grants to the Municipality a non-exclusive, non-transferable right to access and use the Services, provided under any SOW, during the SOW Term (as defined in the applicable SOW), solely for use by authorized Users in accordance with the terms and conditions of this MSA. Such use is limited to the Municipality's internal use for the benefit of the Municipality in the ordinary course of its operations as a municipal corporation. Cycom shall provide to the Municipality the Access Credentials within a reasonable time following the SOW Effective Date of the applicable SOW. The total number of authorized Users shall not exceed the number set forth in the applicable SOW, except as expressly agreed to in writing by the Parties and subject to any appropriate adjustment of the Fees payable hereunder.

6. Services Provided on Municipality's System

If the System is provided by the Municipality (whether as property owned by the Municipality or as property provided to the Municipality by one or more third parties in an arrangement not involving Cycom), and not by Cycom, then this Section 6 shall apply, and Section 5 ("Software as a Service") shall not apply.

1. CityLaw/CountyLaw Software License. Subject to and conditioned on the Municipality's and its authorized Users' compliance with the terms and conditions of this MSA, Cycom hereby grants to the Municipality a non-exclusive, non sublicenseable, non-transferable (except in compliance with Section 24.8 ("Successors and Assignment")) license to use the Software and the Documentation, provided under any SOW, during the SOW Term (as defined in the applicable SOW), solely for use by authorized Users in accordance with the terms and conditions of this MSA. Such use is limited to the Municipality's internal use by the Municipality for the benefit of the Municipality in the ordinary course of its operations as a municipal corporation. The total number of authorized Users shall not exceed the number set forth in the applicable SOW, except as expressly agreed to in writing by the Parties and subject to any appropriate adjustment of the Fees payable hereunder.

7. Accuracy of Municipality Property

The Municipality agrees to be responsible for the accuracy and adequacy of the Municipality Property (as defined in Section 16.2 ("Municipality Property—Definition"), below) which it furnishes or transmits to Cycom for processing or storage. The Municipality represents and warrants that it has the right to upload or otherwise share all Municipality Property that it uploads or shares.

8. Access to Municipality Premises

The use of the Services may require access to the Municipality's premises. The Municipality agrees to provide physical facilities and security as required for proper installation, operation and maintenance of all software and hardware to which the Services apply. If onsite work is required and agreed upon in any SOW, the Municipality will provide Cycom with a work area for Cycom personnel while onsite, which shall include access to any required network, workstations, servers, printers, and Internet connections.

9. Access to Municipality Network and Computers

The Municipality acknowledges that by its use of the Services, it will facilitate the means for remote troubleshooting and support of Cycom's operations, as necessary.

10. Compliance with Network Specifications

The Municipality shall obtain and maintain, at its sole expense, equipment and appropriate telecommunication service adaptable to, compatible with, and suitable for communication with Cycom's network specifications, if any.

11. Term and Termination

1. Term of MSA. The term of this MSA ("Term") shall begin on the Effective Date and, subject to Section 11.4 ("Termination of MSA Requires Termination of SOW"), shall end on the date (the "Expiration Date") that this MSA is terminated (i) by mutual agreement of the Parties, (ii) by either Party for Cause, or (iii) by either Party for convenience upon thirty (30) days written notice to the other Party.

2. Expiration Date. The Expiration Date of this MSA shall be one year (12 months) from the Effective Date of this MSA.

3. Termination of SOW. Termination of all or any part of an SOW shall not terminate this MSA unless otherwise agreed by the Parties in writing. In the event of termination of this MSA or all or any part of an SOW for any reason, the Municipality shall immediately stop using the Services provided under any terminated part of an SOW, and Cycom shall immediately stop work on the terminated portions of all SOWs and shall submit to the Municipality an invoice with supporting information setting forth the applicable fees ("Fees") and other charges for: (i) the Services provided to the Municipality prior to the effective date of such termination, and (ii) in the case of termination by Cycom for Cause or termination by the Municipality for convenience, all non-cancellable commitments and expenses incurred by Cycom prior to the effective date of such termination; and the Municipality agrees to pay Cycom for such invoiced amounts.

4. Termination for Cause. If either Party materially breaches any of its duties or obligations under this MSA or under any SOW, including without limitation in the case of the Municipality, the Municipality 's failure to make payments when due to Cycom for the Services, and such breach is not cured, and the breaching Party is not diligently pursuing a cure to the non-breaching Party's sole satisfaction, within thirty (30) calendar days, after written notice of the breach, then the non-breaching Party may terminate this MSA or any relevant SOW for cause ("Cause") as of a date specified in such notice, or if no date is specified, then upon expiration of such cure period. A Party may terminate this MSA for Cause, effective upon delivery of written notice which shall specify such Cause, if the other Party terminates or suspends its business, or becomes subject to direct control of a trustee, receiver or similar authority, or becomes subject to any bankruptcy or insolvency proceeding under federal or state law.

5. Termination of MSA Requires Termination of SOW. Notwithstanding any other provision herein or in any SOW, the Term of this MSA shall continue while any outstanding SOW remains in effect.

6. Continuation of Liability for Breach. Termination of this MSA shall not act as a waiver of, or as a release from liability for, any breach of this MSA. Termination or expiration of this MSA shall not affect or negate any obligation of either Party (including payment of invoices by the Municipality) to the other arising prior to the date of such termination or expiration.

12. Taxes

Except in the event that the Municipality provides Cycom with a resale exemption certificate or other tax-exempt certificate, the Municipality agrees to pay all sales, use, transaction, excise, VAT or similar taxes and any federal, state or local fees or charges ("Taxes") that may become due in connection with the Municipality's purchase of the Services, other than taxes on the income of Cycom.

13. Confidential Information

As used in this MSA, "Confidential Information" means information of either Cycom or the Municipality which is disclosed under this Agreement in oral, written, graphic, machine recognizable, electronic, sample or any other form by one of us to the other, and which is considered to be proprietary or trade secret by the disclosing party. Confidential Information of Cycom expressly includes, without limitation, the Software Program(s) and Documentation. The Confidential Information of Municipality includes, without limitation, Personally Identifiable Information and Municipality content. Confidential Information shall not include information which the party receiving the information can demonstrate: (i) was in the possession of or known by it without an obligation of confidentiality prior to receipt of the information, (ii) is or becomes general public knowledge through no act or fault of the party receiving the information, (iii) is or becomes lawfully available to the receiving party from a third party without an obligation of confidentiality, or (iv) is independently developed by the receiving party without the use of any Confidential Information. Confidential Information includes, without limitation:

1. when Cycom is the Disclosing Party, the Software and the Documentation, all delivery methods for the activities and software and other deliverables provided by Cycom in connection with the
   Services, all information and materials related to Cycom business methods, and all Cycom information related to sales, profits, organizational structure and restructuring, new business initiatives, finances, services and products, and product designs; and
2. when either Cycom or the Municipality is the Disclosing Party, information relating to the Disclosing Party's planned or existing computer systems and systems architecture, software, hardware, networks, and databases and database management systems, any confidential information of third parties with which the Disclosing Party conducts business, and any Trade Secrets of the Disclosing Party.

As used in this MSA, "Trade Secret" means trade secret as that term is defined by the federal Defend Trade Secrets Act, 18 U.S.C. § 1836 et seq., as it may be amended from time to time, including without limitation software or computer code.

The Municipality acknowledges and agrees that the object code of the Software is a Trade Secret of Cycom. The Receiving Party may use Confidential Information only in connection with the transactions contemplated by this MSA and the associated SOWs.

The Receiving Party shall take all reasonable measures to avoid disclosure, dissemination or unauthorized use of Confidential Information, including, at a minimum, those measures it takes to protect its own confidential information of a similar nature.

The Parties agree to advise their respective employees, agents, and subcontractors of their obligations to keep all Confidential Information confidential, and to require them to do so.

The Receiving Party shall notify the Disclosing Party immediately upon discovery of any unauthorized use or disclosure of Confidential Information by the Receiving Party.

The Receiving Party shall cooperate with the Disclosing Party in every reasonable way to help the Disclosing Party regain possession of such Confidential Information and to prevent its further unauthorized use.

If either Party is uncertain at any time whether particular information is considered to be Confidential Information of the other Party, it shall promptly contact the other Party for clarification. Each Party's obligations under this MSA with respect to another Party's Confidential Information that is not a Trade Secret shall survive for a period of two (2) years following the date of termination of this MSA. The obligations hereunder to maintain the confidentiality of Trade

14. Non-Solicitation

During the Term and for a period of twelve (12) months following the Expiration Date, neither Party shall,
without the written permission of the other Party, directly or indirectly (i) solicit, employ or retain, or have or cause any other person or entity to solicit, employ or retain, any person who is employed or subcontracted by the other Party or was employed or subcontracted by the other Party during the Term; (ii) encourage any such person not to devote his or her full business time to the other Party; or (iii) in any other manner interfere with the business relationship between the other Party and its employees or subcontractors.
This section shall survive the termination of this MSA.

15. Equitable Relief

In addition to any other remedies and damages available, each Party acknowledges and agrees that in the event of any breach or threatened breach of Sections 13 ("Confidential Information") or 14 ("Non- Solicitation") of this MSA: (i) notwithstanding the existence of any mediation or arbitration agreement between the Parties, the nonbreaching Party has the right to file a civil action; and (ii) the nonbreaching Party may immediately seek enforcement of Sections 13 ("Confidential Information") and 14

("Non-Solicitation") of this MSA by means of specific performance or temporary, preliminary and permanent injunctive relief without the necessity of proving inadequacy of legal remedies or irreparable harm, or posting bond. This section shall survive the termination of this MSA.

16. Ownership of Software and Other IP

1. Cycom Property Definition. "Cycom Property" means: (i) any proprietary technology which was developed or acquired by Cycom, or by any of its licensors and suppliers, prior to the Effective Date of this MSA, including without limitation the Software and the Documentation, other software (in source and object forms) and class libraries and objects and executables, hardware designs, algorithms, user interface designs, architecture, network designs, database and database management designs, and documentation (both printed and electronic); (ii) all versions and releases of and updates to the Software that are developed or acquired by Cycom after the Effective Date of this MSA and not transferred by Cycom to any other party, as well as any proprietary technology developed or acquired by Cycom's licensors and suppliers after the Effective Date of this MSA; (iii) any Trade Secret, patent, copyright or trademark rights, or other similar intellectual property rights, owned by Cycom or by any of its licensors and suppliers; and (iv) any derivatives, improvements, enhancements or extensions of any of the foregoing that are conceived, reduced to practice or developed in the course of the performance of the Services, by either Party, that are not uniquely applicable to the Municipality and are not developed specifically and exclusively for the Municipality, or that have general applicability in the art.

2. Municipality Property Definition. "Municipality Property" means: (i) Municipality folders, files, documents, logs, database information, and similar data that Cycom maintains on behalf of the Municipality; (ii) Municipality credentials, network account information, web portal login information, administrative passwords, and similar information; (iii) third-party software licensed to the Municipality by its licensors and suppliers in an arrangement not involving Cycom; and (iv) the System if provided by the Municipality (whether as property owned by the Municipality or as property provided to the Municipality by one or more third parties in an arrangement not involving Cycom) and not by Cycom.

3. Ownership of Cycom Property. All Cycom Property shall remain the sole and exclusive property of Cycom or its licensors or suppliers. Except as specifically set forth herein, this MSA does not grant the Municipality any rights to the Cycom Property. Any Cycom Property provided in connection with the Services is licensed or sublicensed to the Municipality, or provided to the Municipality for its limited access and use, only in

connection with the Services, and not for unlimited use.

4. Ownership of Municipality Property. Ownership of Municipality Property remains with the Municipality or its licensors and suppliers and shall not be deemed the property of Cycom or any other party; provided that, the Municipality grants Cycom a limited license to access, use and modify Municipality Property as reasonably necessary to enable Cycom to provide the Services. Cycom shall not be required to provide access to Municipality Property to parties

5. Survival of Ownership of Software and Other . This section shall survive the termination of this MSA.

17. Protection of IP

1. Infringement Claims By Third Parties. In the event that the Software or the Documentation, as delivered or as modified by Cycom, becomes, or in the opinion of Cycom is likely to become, the subject of a claim of infringement of any Trade Secret, patent, copyright or trademark rights, or other similar intellectual property rights, owned by any third party, then Cycom may, at its option and expense, either: (i) procure for the Municipality the right to continue to use the Software and the Documentation as contemplated in this MSA; or (ii) replace or modify either or both of the Software and the Documentation, or modify the use of either or both, in order to make their use under this MSA non-infringing. If neither option is reasonably available to Cycom, then this Agreement may be terminated for convenience at the option of either party pursuant to Section 11.1 ("Term of MSA") above.

2. Protection of Cycom Patents. Cycom agrees that it will, during the Term of this MSA, use reasonable commercial efforts to maintain, protect and defend the registration of any patent registered with the United States Patent and Trademark Office, where such patent gives Cycom any patent rights in the Software or the Documentation (any such patent a "Patent"). The Municipality agrees to execute any further documents and to perform any further acts, at Cycom's expense, as may be necessary to assist Cycom in maintaining, protecting and defending such registration of any such Patent.

18. Restrictions on the Use of the Services

1. Use for Lawful Purposes. The Municipality represents, undertakes and warrants to Cycom that the Municipality will not use the Services in a manner that violates any applicable laws, rules or regulations, including but not limited to, privacy and data protection laws and regulations, and will not authorize or permit any other person to use the Services in any such manner. The Municipality agrees that it will not:

   a. copy (except for normal security backup purposes), modify, or create derivative works or improvements of the Services;

   b. rent, lease, lend, sell, sublicense, assign, distribute, publish, or transfer any part of the Services to any person;

   c. reverse engineer, disassemble, decompile, decode, adapt, or otherwise attempt to derive or gain access to the source code of the Software, in whole or in part;

   d. bypass or breach any security device or protection used by the Services, or access or use the Services other than by an authorized User through the use of his or her own then valid Access Credentials;

   e. input, upload, transmit, or otherwise provide to or through the Services, any virus, worm, malware, or other harmful computer code;

   f. damage, destroy, disrupt, disable, impair, interfere with, or otherwise impede or harm in any manner the Services, the System if provided by Cycom, or Cycom's provision of services to any third party, in whole or in part;

   g. remove, delete, alter, or obscure any specifications, warranties, or disclaimers, or any copyright, trademark, patent, or other intellectual property or proprietary rights notices, from any component of the Services, including any copy thereof;

   h. access or use the Services in any manner or for any purpose that infringes, misappropriates, or otherwise violates any intellectual property rights or other rights of any third party;

   i. access or use the Services for purposes of competitive analysis of the Services, for purposes of the development, provision, or use of a competing software service or product, or for any other similar purpose that is to the commercial disadvantage or detriment of Cycom; or

   j. otherwise access or use the Services beyond the scope of the authorization granted under this MSA by Cycom.

Unauthorized Installation. Cycom reserves the right to interrupt or restrict the Services without notice to the Municipality if Cycom detects evidence that the Municipality has attempted any software installation, or has placed executable program code, on Cycom systems without explicit knowledge of, or written permission from, Cycom. The Municipality agrees to cooperate with Cycom in

any investigation relating to software or code installations and to use any reasonable prevention measures prescribed by Cycom. The Municipality shall be solely liable for any and all damages resulting from any such unauthorized software or code implementation by the Municipality.

2. Fraud or Abuse. Cycom reserves the right to interrupt or restrict the Services without notice to the Municipality if Cycom suspects fraudulent or abusive activity related to the Municipality's use of the Services. The Municipality agrees to cooperate with Cycom in any fraud investigation and to use any reasonable fraud prevention measures prescribed by Cycom. The Municipality shall be solely liable for any and all damages resulting from the Municipality's fraudulent or abusive usage or activity.

3. Protection of Cycom Property. Cycom reserves the right to intercept and disclose any sessions being served by Cycom's facilities in order to protect Cycom's rights or property. If Cycom reasonably determine that the security of the Services or Cycom infrastructure may be compromised due to hacking attempts, denial of service attacks, or other malicious activities, Cycom may temporarily suspend the Services.

4. Municipality Accounts. The Municipality is solely responsible for (i) all use of the Services by the Municipality and its users, (ii) maintenance of lawful bases for the collection, use, processing and transfer of data by the Municipality, and (iii) provision of notices and obtaining of consent as legally required in connection with the Services. The Municipality agrees to keep its usernames, passwords and authentication tokens confidential. Cycom is not liable for any loss incurred by the Municipality caused by unauthorized third parties using the Municipality's accounts. The Municipality agrees to notify Cycom promptly in the event of its discovery of any unauthorized access to the Services or other security breach. The Municipality represents, warrants, and covenants to Cycom that, as received by Cycom from the Municipality, the Municipality Property will not infringe, misappropriate, or otherwise violate any Trade Secret, patent, copyright or trademark rights, or other similar intellectual property rights, or any privacy rights, of any third party.

5. Survival of Restrictions on Use of the Services. The provisions of this Section 18 ("Restrictions on Use of the Services") shall survive the termination of this MSA.

19. Warranties, Disclaimers, and Municipality Responsibilities

1. Third-Party Hardware and Software. With respect to any third-party hardware or software sold, distributed, licensed or supplied by Cycom in connection with the Services, to the extent permitted by the manufacturer or licensor of such hardware or software, Cycom will pass through to the Municipality all product warranties provided by the manufacturer or licensor.

2. Disclaimers – In General. THE SERVICES, INCLUDING ACTIVITIES AND DELIVERABLES, ARE PROVIDED "AS-IS," WITHOUT ANY WARRANTIES OF ANY KIND EXCEPT AS SPECIFICALLY DESCRIBED IN THIS MSA. CYCOM EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THE MUNICIPALITY AGREES THAT CYCOM SHALL NOT BE RESPONSIBLE FOR ANY FAILURES OF SOFTWARE OR EQUIPMENT THAT MAY OCCUR AS A DIRECT OR INDIRECT RESULT OF PROVISION OF THE SERVICES BY CYCOM, AND
CYCOM DOES NOT REPRESENT, WARRANT, OR COVENANT THAT THE SERVICES OR ANY INCLUDED DELIVERABLES OR ASSOCIATED SOFTWARE OR EQUIPMENT OR COMPONENTS, OR THE SYSTEM, WILL: (I) MEET THE MUNICIPALITY'S REQUIREMENTS; (II) BE UNINTERRUPTED OR AVAILABLE AT ANY PARTICULAR TIME FROM ANY PARTICULAR LOCATION; (III) BE ERROR-FREE; (IV) NOT INFRINGE UPON THE RIGHTS OF ANY THIRD PARTY; (V) IN THE CASE OF SOFTWARE, BE COMPATIBLE WITH THE MUNICIPALITY'S HARDWARE OR OTHER SOFTWARE; OR (VI) BE FREE FROM UNAUTHORIZED USERS OR HACKERS. WHILE CYCOM USES ENCRYPTION TECHNOLOGY IN THE PROVISION OF THE SERVICES, CYCOM DOES NOT GUARANTEE OR WARRANT THE SECURITY OF ANY NETWORK CONNECTION CREATED OR MAINTAINED PURSUANT TO THE PROVISION OF THE SERVICES. CYCOM MAKES NO WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM USE OF THE SERVICES.

3. Disclaimers – Municipality Responsibilities. The Municipality shall be solely responsible, and in no event shall Cycom be responsible or liable in any way, for any losses, liabilities or damages caused by or related to: (i) design specifications or instructions provided by the Municipality or the Municipality's representative; (ii) the Municipality's failure to fulfill its responsibilities under this MSA or any SOW;
(iii) the failure of anyone other than Cycom or its subcontractors to comply with written instructions or recommendations from Cycom or its subcontractors; (iv) any alteration or improper installation, storage, handling, use or maintenance or repair of any part of any deliverable under the Services by anyone other than Cycom or its subcontractors; (v) anything external to any deliverable under the Services at the Municipality's site, including but not limited to building deficiency, power surge, fluctuation or failure, or air conditioning failure; (vi) movement of any deliverable under the Services
installed at the Municipality's site from the location where it was installed by Cycom; or (vii) any other
cause beyond Cycom's reasonable control. In addition, the Municipality acknowledges that

the use of any computer network entails a risk of loss of stored data, that industry standards dictate the

Municipality's systematic use of equipment for comprehensive backup of data, and that even the systematic use of backup equipment cannot guarantee against the loss of data; accordingly, (A) the Municipality is solely responsible for maintaining and backing up all data and software stored on its computers and storage media before ordering the Services, and (B) the Municipality assumes all risk of loss of its stored data and software in any way related to or resulting from the use of any network or backup system installed or created for the Municipality hereunder, or from the provision of the Services hereunder, and hereby releases Cycom from any liability for loss of such data.

4. Survival of Warranties and Disclaimers. The provisions of this Section 19 ("Warranties; Disclaimers; Municipality Responsibilities") shall survive the termination of this MSA.

20. Indemnification

1. Indemnification of Cycom By the Municipality. The Municipality shall indemnify, defend and hold harmless Cycom, its affiliates, and their respective directors, officers, employees and agents (the "Cycom Indemnified Parties"), from and against any and all claims, actions, losses, damages, costs or expenses (including reasonable attorneys' and experts' fees) arising out of or resulting from any breach by the Municipality of Sections 4.2 ("Unlicensed Software"), 7 ("Accuracy of Municipality Property"), 16.3 ("Ownership of Cycom Property"), or 18 ("Restrictions on Use of the Services"). The Cycom Indemnified Parties will notify the Municipality of any claim for which the Municipality is responsible, and will reasonably cooperate with the Municipality to facilitate the defense of such claim. The Cycom Indemnified Parties may select and employ counsel at their own expense with respect to the defense of a claim; provided that, if counsel is employed due to a conflict of interest or because the Municipality does not assume control of the defense, the Municipality shall bear such expense. The Municipality shall not admit liability or enter into any settlement of a claim that might adversely affect a Cycom Indemnified Party's rights or interests without the Cycom Indemnified Party's prior written consent, which may be withheld in the Cycom Indemnified Party's sole discretion.

2. Indemnification of the Municipality By Cycom. Cycom shall indemnify, defend and hold harmless the Municipality, its affiliates, and their respective directors, officers, employees and agents (the "Municipality Indemnified Parties"), from and against any and all claims, actions, losses, damages, costs or expenses (including reasonable attorneys' and experts' fees) arising out of or resulting from any claim of infringement of any Trade Secret, patent, copyright or trademark rights, or other similar intellectual property rights asserted against the Municipality by virtue of the Municipality's use of the Services as delivered by Cycom and used according to Cycom's instructions; provided that, CYCOM shall have no liability for, and no obligation to indemnify, defend or hold harmless any Municipality Indemnified Party with respect to, any claim of infringement of any Trade Secret, patent, copyright or trademark rights, or other similar

intellectual property rights, based on the Municipality's unauthorized use of, or combination of any component of the Services with, products not supplied by Cycom as part of the Services. The Municipality Indemnified Parties will notify Cycom of any claim for which Cycom is responsible, and will reasonably cooperate with Cycom to facilitate the defense of such claim. The Municipality Indemnified Parties may select and employ counsel at their own expense with respect to the defense of a claim; provided that, if counsel is employed due to a conflict of interest or because Cycom does not assume control of the defense, Cycom shall bear such expense. Cycom shall not admit liability or enter into any settlement of a claim that might adversely affect a Municipality Indemnified Party's rights or interests without the Municipality Indemnified Party's prior written consent, which may be withheld in the Municipality Indemnified Party's sole discretion.

Survival of Indemnification. The provisions of this Section 20 ("Indemnification") shall survive the termination of this MSA.

1. Nonwaiver of Rights. Indemnitees do not and shall not waive any rights that they may possess against Cycom because the acceptance by Municipality, or the deposit with the Municipality of any insurance policy or certificate required pursuant to this Agreement.

2. Waiver of Right of Subrogation. Cycom on behalf of itself and all parties claiming under or through it, hereby waives all rights of subrogation and contribution against the Indemnitees.

21. Limitations of Liability

1. Exclusions. NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED HEREIN, IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES (INCLUDING FOR LOST PROFITS, COSTS OF DELAY, FAILURE OF DELIVERY, BUSINESS INTERRUPTION, LOSS OF USE OF THE SYSTEM, MALICIOUS ATTACKS, SOFTWARE INCOMPATIBILITIES, UNAUTHORIZED INTRUSIONS, OR LOST, DAMAGED OR INADVERTENTLY DISCLOSED DATA OR DOCUMENTATION, OR LIABILITIES TO THIRD PARTIES ARISING FROM ANY SOURCE), REGARDLESS OF THE NATURE OF THE CLAIM, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING LIMITATION SHALL APPLY WITHOUT REGARD TO WHETHER ANY PROVISIONS OF THIS MSA HAVE BEEN BREACHED, HAVE PROVEN INEFFECTIVE, OR HAVE FAILED OF THEIR ESSENTIAL PURPOSE.

2. Limitations. THE CUMULATIVE, AGGREGATE LIABILITY OF EACH PARTY FOR ALL CLAIMS ARISING FROM OR RELATING TO THIS MSA, WHETHER IN CONTRACT, TORT, STRICT LIABILITY, OR ANY OTHER LEGAL THEORY, SHALL NOT EXCEED (I) IN THE CASE OF CYCOM, THE TOTAL AMOUNT OF FEES PAID TO CYCOM BY THE MUNICIPALITY, AND (II) IN THE CASE OF THE MUNICIPALITY, THE TOTAL AMOUNT OF FEES PAID AND PAYABLE TO CYCOM BY THE MUNICIPALITY; EACH UNDER THE APPLICABLE ORDER OR SOW RELATED TO THE CLAIM DURING THE TWELVE (12)-MONTH PERIOD IMMEDIATELY PRECEDING THE

DATE SUCH LIABILITY AROSE. PROVIDED, HOWEVER, THAT THE FOREGOING LIMITATION SHALL NOT APPLY TO: (A) DAMAGES CAUSED BY A PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT; OR (B) A PARTY'S BREACH OF ITS OBLIGATIONS UNDER SECTIONS 13 ("CONFIDENTIAL INFORMATION") OR 14 ("NON-SOLICITATION") OF THIS MSA

3. Survival of Limitations of Liability. The provisions of this Section 21 ("Limitations of Liability") shall survive the termination of this MSA.

22. Subcontractors

Cycom shall not assign or sublet to any other party without the prior written approval of Municipality which approval may be withheld in the Municipality's sole and absolute discretion. In the event that the Municipality, in writing, approves any assignment or subletting of this Agreement or the retention of subcontractors by Cycom, Cycom shall provide to the Municipality upon request copies of each and every subcontract prior to the execution thereof by Cycom and subcontractor. Any attempt by Cycom to assign any or all of its rights under this Agreement without first obtaining the Municipality's prior written consent shall constitute a material default under this Agreement.

23. General

1. Notice. All notices permitted or required by this MSA shall be in writing and shall be deemed to have been duly given: (a) on the date personally delivered; (b) three (3) business days after being mailed via United States Postal Service, certified and return receipt requested; or (c) one (1) business day after being sent by a nationally recognized overnight courier. Notices may also be sent by email; provided that, a notice sent by email shall be deemed effectively given only if the recipient, by an email sent to the email address for the sender or by a notice delivered by another method in accordance with this section, acknowledges having received that email, with an automatic "read receipt" not constituting acknowledgment of an email for purposes of this section. All notices permitted or required by this MSA shall be addressed as shown below, or as may later be designated by the addressee Party.

The Municipality:

Jennifer Espinoza, Law Office Manager
City of Redondo Beach
415 Diamond Street, Redondo Beach, CA 90277
jennifer.espinoza@redondo.org

Cycom:

Cycom Data Systems, Inc.
P.O. Box 802
Richmond, KY 40476-0802
accounts@cycominc.com

2. Independent Contractors. This MSA shall not create a joint venture, partnership, fiduciary relationship or other formal business relationship or entity of any kind, or an obligation to form any such relationship or entity. Cycom shall perform the Services as an independent contractor. Neither Party shall have the authority to bind the other, except as specifically granted in this MSA.

3. Third Party Beneficiaries. For the purposes of Section 23 ("Insurance"), and Cycom's obligations thereunder, non-Parties who are protected by, named as additional insureds under, or made the subject of waivers of subrogation under, Cycom's insurance ("Additional Insureds") under the provisions of Section 23 ("Insurance") are third-party beneficiaries of this MSA in accordance with its terms. Other than as provided for in Section 23 ("Insurance"), this MSA is for the sole benefit of the signatories hereto and their permitted successors and assigns. Nothing, express or implied, in this MSA is intended to create or be construed to create any rights of enforcement in any persons or entities who are not signatories to this MSA.

4. Marketing. Cycom may include the Municipality's name in its list of clients, which may be provided to prospective Cycom clients.

5. Construction. This MSA is the result of negotiations between, and has been reviewed by, each of the Parties hereto and their respective counsel, if any; accordingly, this MSA shall be deemed to be the product of both of the Parties hereto, and no ambiguity shall be construed in favor of or against either of the Parties hereto.

6. Entire Agreement. This MSA, together with the exhibits hereto and the documents specifically described herein as containing additional terms of this MSA, constitutes the entire agreement between the Parties relating to the matters discussed herein and may be amended or modified only with the mutual written consent of the Parties.

7. Severability. The invalidity or unenforceability of any provision of this MSA shall not affect the validity or enforceability of any other provision of this MSA.

8. Successors and Assignment Subject to the limitations set forth in this MSA, this MSA shall inure to the benefit of and be binding upon the Parties and their respective successors and assigns. This

MSA shall not be assigned, in whole or in part, by a Party without the prior written consent of the other Party, which shall not be unreasonably withheld; provided that, either Party may assign this MSA in its entirety without the consent of the other Party pursuant to a merger, acquisition, or sale of substantially all the assets of that portion of the Party's business primarily responsible for performing under or exercising rights under this MSA.

9. No Waiver. Any failure by either Party to enforce the other Party's strict performance of any provision of this MSA shall not constitute a waiver of its right to substantially enforce such provision or any other provision of this MSA.

10. Governing Law. The validity, interpretation, construction and performance of this MSA, and all acts and transactions pursuant hereto and the rights and obligations of the Parties hereto shall be governed, construed and interpreted in accordance with the laws of the state of California, without giving effect to principles of conflicts of law. For purposes of litigating any dispute that may arise directly or indirectly from this MSA, whether in contract, tort, or otherwise, the Parties hereby submit and consent to the exclusive jurisdiction of the state or federal courts located in Los Angeles County, California, and agree that any such litigation shall be conducted only in the courts of the state of California located in the County of Los Angeles and no other courts.

11. Waiver of Jury Trial; Attorney Fees. Each Party irrevocably and unconditionally waives any right it may have to a trial by jury in respect of any legal action arising out of or relating to this MSA or the transactions contemplated hereby. In the event that any legal action is instituted by either Party to enforce any of the terms and provisions of this agreement, the prevailing Party, as determined by the court, shall be entitled to reasonable attorney fees, costs and expenses, in such amounts as may be determined by the court.

12. Force Majeure. Neither Party shall be liable for failure to perform or delay in performance hereunder if such failure or delay is due to fire, storm, flood, war, insurrection, labor dispute, embargo, epidemic or quarantine restriction, complete or partial government shutdown, national or regional shortage of adequate power or telecommunications or transportation, delay by supplier of materials or services, or any act of God or other cause or contingency beyond such Party's reasonable or foreseeable control ("Force Majeure Event"). Upon the occurrence of any such failure to perform or delay in performance due to a Force Majeure Event, the Parties agree to renegotiate in good faith the terms and schedule for the provision of the Services.

13. Mediation and Arbitration.

a. Mediation. The Parties will attempt in good faith to resolve any claim or controversy arising out of or relating to the interpretation or performance of this MSA by negotiations between the Parties. In the event that any dispute cannot be resolved by negotiations between the Parties, then any controversy or claim arising out of or relating to this MSA shall be attempted to be settled by mediation which, unless the Parties agree otherwise in writing, shall be in accordance with the Mediation Procedures of the American Arbitration Association currently in effect. Any such mediation shall take place in Los Angeles County, California, or remotely via videoconference upon agreement by both Parties.

b. Arbitration. In the event that the dispute is not resolved through mediation, the Parties shall endeavor to resolve the dispute by arbitration in accordance with the Arbitration Rules of the American Arbitration Association (the "AAA") currently in effect. Any such arbitration shall take place in Los Angeles County in the state of California. Notwithstanding the foregoing, either Party has the right to file a civil action in the event that such Party deems it necessary to seek an equitable remedy, as stipulated in Section 15 ("Equitable Relief"), above. The following provisions shall apply to any arbitration under this section:

i. To instate an arbitration under this section, a notice of arbitration must be provided to the opposing Party pursuant to Section 24.1 ("Notice") above.

ii. The arbitration shall be conducted by a single, neutral arbitrator. Within seven (7) days of the effective date of the notice of arbitration, the Parties shall mutually agree upon an arbitrator. If the Parties cannot agree upon the identity of the arbitrator, the American Arbitration Association shall provide the Parties with a list of five (5) qualified arbitrators, the Parties shall rank these candidates numerically, and the highest mutually ranked candidate shall be selected to preside over the dispute.

iii. A hearing shall be held within ninety (90) days of the effective date of the notice of arbitration. Such hearing shall last no more than three (3) business days. Within fourteen (14) days of the conclusion of the hearing, the arbitrator shall issue an award and a grant of non-monetary remedy or relief, if any.

iv. The arbitration shall not require any personal appearance by the Parties or witnesses unless otherwise agreed by the Parties. To the extent that the arbitrator deems reasonable, the arbitrator shall conduct hearings, if any, by teleconference or videoconference, rather than by personal appearances.

v. The arbitrator shall have the authority to grant motions dispositive of all or part of any claim. The arbitrator shall have the authority to award monetary damages, and to grant any non- monetary remedy or relief available to any party under applicable law, the Arbitration Rules of the AAA, and the terms of this MSA.

vi. The arbitrator shall issue a written award and statement of decision describing the essential findings and conclusions on which the award is based, including the calculation of any damages awarded. The arbitrator shall have the same authority to award relief on an individual basis that a judge in a court of law would have.

vii. The prevailing Party, as determined by the arbitrator, may be awarded all reasonable costs and fees of the arbitration including, without limitation, the arbitrator's fees and reasonable attorneys' fees, at the sole discretion of the arbitrator.

viii. In deciding any arbitration under this section, the arbitrator shall apply the substantive law of
the state of California exclusive of its laws governing conflicts of law. However, matters relating to the enforceability of this section, to the procedures to be followed in carrying out any arbitration, and to any award granted under this section shall be governed by the Federal Arbitration Act, 9 U.S.C. §§ 1-16. Arbitrable matters shall include: (A) matters concerning the scope, construction and enforcement of this section; and (B) material matters that arise under or relate to this MSA, including the applicability of the laws of the state of California to any provision of this MSA.

ix. Any judgment upon the award rendered in any arbitration may be entered in any court of competent jurisdiction.

14. Data Privacy. Cycom shall employ security measures in accordance with Cycom's data privacy and security policy as amended from time to time, a current copy of which is attached hereto as **EXHIBIT B_____.** Cycom maintains a data breach plan in accordance with the criteria set forth in Cycom's Privacy and Security Policy, and shall implement the procedures required under such data breach plan upon the occurrence of any data breach as defined in such Privacy and Security Policy. Should any terms within Exhibit B conflict with the terms of this Agreement, the terms of this Agreement shall govern.

DATA RETENTION AND BACKUPS: For cloud data (documents, software, database), Cycom shall maintain consistent, regular, and validated backups of Municipality content and Confidential Information imported into the Software Program(s) in strict accordance with _Microsoft Azure_ cloud network's

policies and procedures. Upon written request, Cycom shall provide Municipality with the current retention and backup policies and procedures.

Municipality is responsible for all backups and data retention for data (documents, software, databases) which reside on Municipality assets.

AUDITS AND SECURITY: Cycom is committed to maintaining the security of the Municipality's content and Confidential Information within the Software Program(s). Cycom shall maintain the Software Program(s) in a secure manner consistent with industry best practices and in accordance with Microsoft Azure cloud policies and procedures. Cycom shall conduct regular security audits of the Software Program(s) to protect their integrity and security. Municipality is responsible for protecting and safeguarding usernames and passwords on its end. Both parties agree to cooperate in maintaining the overall security of the system. Cycom shall promptly notify Municipality of any security breaches or unauthorized access to Municipality content or Confidential Information, and shall take all necessary steps to mitigate any potential harm.

DATA TRANSMISSION: Cycom ensures that all data transmitted to and from the Software Program(s) is encrypted using a minimum of 256-bit SSL encryption with digital certificates issued by an internationally recognized domain registrar and certificate authority. Data-at-rest encryption shall be through_Microsoft Azure standard practice.

Cycom shall use 2048bit SSL Encryption Key to meet the FIPS 140-2 Compliant requirements. Cycom maintains security policies and practices which are in compliance with SOC2 Type Certification. See Exhibit B. Cycom shall maintain and use said security policies and practices which are in compliance with SOC2 Type Certification for the duration of this Agreement. Should any terms within Exhibit B conflict with the terms of this Agreement, the terms of this Agreement shall govern.

DATA LOCATION: Cycom shall maintain the Software Program(s), Municipality content, and Confidential Information of Municipality in a SAS 70/SSAE 16 certified data facility.
All data is stored in the U.S. and is stored in Microsoft Azure US Based cloud facilties .

DATA DELETION: Upon termination of the agreement or upon Municipality's written request, Cycom shall securely delete all Municipality content and Confidential Information from its systems and provide a certificate of destruction to the Municipality within thirty (30) days of Municipality's written request, confirming the deletion.

ACCESS CONTROL: Cycom shall implement strict access control measures to ensure that only authorized personnel have access to Municipality content and Confidential Information. All access shall be logged and subject to regular review.

DATA BREACH: In the event of a data breach or security incident, Cycom shall promptly notify the Municipality within 24 hours and take all necessary steps to mitigate any potential harm

COMPLIANCE WITH LAWS:

Cycom shall comply with all applicable data protection and privacy laws, including but not limited to the California Consumer Privacy Act ("CCPA") and any other relevant legislation.

15. Conflict of Interest. Cycom covenants that no officer, member or employee of the Municipality and no other public official who exercises any functions or responsibility in

the review, approval or

carrying out of this MSA has any personal or financial interest, direct or indirect, in this MSA.

16. Counterparts. This MSA may be executed in any number of counterparts, each of which when so executed and delivered shall be deemed an original, and all of which together shall constitute one and the same agreement.

17. Survival of General Provisions. The provisions of this Section 24 ("General") shall survive the termination of this MSA

StatementofWork(SOW)

Exhibit A

This Statement of Work ("SOW") is entered into, to be effective as of the Effective Date of the Master Services Agreement ("MSA"), by and between Cycom Data Systems, Inc., a California corporation having a mailing address at P.O. Box 802, Richmond, KY 40476-0802 ("Cycom") and the City of Redondo Beach, a municipal corporation having a principal office address at 415 Diamond Street, Redondo Beach, CA 90277 (the "Municipality"), and specifies the particular Services, including activities and deliverables, described in more detail below, to be performed hereunder by Cycom for the Municipality. Either of Cycom and the Municipality may be referred to herein as a Party, and together as the "Parties."

Recitals

Whereas, Cycom has agreed to provide certain Services to the Municipality, including activities and deliverables, described in more detail below, all on the terms and conditions set forth herein.

Now, therefore, the Parties agree as follows:

1. Incorporation into MSA

This SOW, including all exhibits attached to this SOW, shall be incorporated into and made a part of and governed by the terms of that certain Master Services Agreement entered into by and between the Municipality and Cycom, effective as of the Effective Date stated therein, and as amended (the "MSA"). Capitalized terms used, but not otherwise defined, in this SOW shall have the meanings ascribed to them in the MSA.

2. Term of SOW

The initial term of this SOW ("SOW Initial Term") shall begin on the SOW Effective Date and shall end on the date ("SOW Initial Term Expiration Date") that is Twelve (12) Months from the SOW Effective Date. This SOW may be terminated (i) by mutual agreement of the Parties, (ii) by either Party for Cause, or (iii) by either Party for convenience upon sixty (60) days written notice to the other Party. If the System is provided by Cycom, and not by the Municipality, then upon any termination of this SOW, Cycom shall retain the Municipality's data until the earlier of (A) sixty (60) days, or (B) such time as Cycom receives written confirmation from the Municipality that the Municipality has downloaded and saved its data; and the Municipality agrees that Cycom may delete the Municipality's data after such time.

3. Change Management

The terms and conditions of this SOW, including without limitation the scope of the Services, applicable timelines and due dates, Fees and other charges, and items provided, may be changed only upon execution by the Parties of a written change order ("Change Order") that references this SOW and that specifies such change. Either Party may request a change, and both Parties agree to negotiate in good faith any requested changes. In the event of a conflict between the terms and conditions set forth in a Change Order and those set forth in this SOW or in a previously executed Change Order, the terms and conditions of the most recent Change Order shall prevail.

4. Specific Services, Payment and Fees, and Acceptance of Services

New or Additional Services; Expanded Scope. Any new or additional Services, including any new or additional hardware or software or other deliverables, other than those contracted for by the Municipality on the SOW Effective Date, may be obtained by the Municipality at the then-current price.

Invoicing. Cycom shall bill by invoice to the Municipality the sums due pursuant to this SOW. Cycom will send all invoices electronically to the Municipality's Account Holder (as listed in Section 5.2 ("Contact Persons for Municipality") below), provided that Cycom may in its sole discretion also send any invoice by mail to a billing address supplied by the Municipality. Each invoice shall include:
(a) the Cycom invoice number; (b) a description of the Services for which an amount is due; (c) any adjustments made to Fees; (d) the Fees or portion thereof, and any other charges that are due; (e) Taxes, if any; (f) credits provided to the Municipality by Cycom, if any; (g) all pass-through costs and expenses associated with provision of the Services; and (h) the total amount due.

Payment. Payment shall be due sixty (60) days after the Municipality receives an invoice from Cycom. The date of receipt by the Municipality of any invoice sent to the Municipality by Cycom shall be determined according to the provisions of Section 23.1 ("Notice") of the MSA, provided that the Municipality may supply a billing address or email address that is different from the address or email address of the Municipality listed in Section 23.1 ("Notice") of the MSA. The Municipality agrees to make payment on any invoiced charges. All amounts payable to Cycom under this SOW shall be paid by the Municipality to Cycom in full without any setoff, recoupment, counterclaim, deduction, debit, or withholding for any reason (other than service credits that may be issued to the Municipality by

Cycom, or any deduction or withholding of tax as may be required by applicable law). All payments are non-refundable unless otherwise agreed in a writing signed by both Parties. The Municipality may pay by credit card, or may send payments by check to:

Finance Department
Cycom Data Systems, Inc.
P.O. Box 802
Richmond, KY 40476-0802

Acceptance of Services by Municipality. Following delivery to the Municipality by Cycom of any invoice for any of the sums due pursuant to this SOW, the Municipality shall have ten (10) business days to object in writing to any of the contents of such invoice. Failure by the Municipality to so object shall constitute acceptance by the Municipality of those portions of the Services to which such contents of such invoice apply.

Survival of Payment Obligations. This Section 4 ("Specific Services; Payment and Fees; Acceptance of Services") shall survive the termination of this SOW and the MSA.

Exhibit A-2-a

This CityLaw (Municipality Hosted) Rider ("Exhibit A-2-a") is entered into, to be effective as of the SOW Effective Date, by and between Cycom and the Municipality, and specifies certain of the particular Services, including activities and deliverables, described in more detail below, to be performed hereunder by Cycom for the Municipality.

1. Incorporation into SOW

This Exhibit A-2-a shall be incorporated into and made a part of and governed by the terms of that certain Statement of Work, effective as of the Effective Date stated therein, entered into by and between the Municipality and Cycom, and as amended (the "SOW"). Capitalized terms used, but not otherwise defined, in this Exhibit A-2-a shall have the meanings ascribed to them in the SOW or the MSA.

2. Service Details and Fees

The Municipality agrees to purchase from Cycom, and Cycom agrees to sell to the Municipality, a Software license for the CityLaw Software developed and provided by Cycom, as well as certain other associated Services. The following terms shall govern the Services provided under this Exhibit A-2-a:

Software	CityLaw
Rights of Access and Use	The details of the Municipality's right to access and use the CityLaw Software developed and provided by Cycom, as hosted on the System provided by Cycom, are given in Section 6.1 ("CityLaw/CountyLaw Software License") of the MSA.
Term of Rights of Access and Use	Beginning on the Effective Date and ending Twelve (12) Months after.

Limitations on Fee Increase	Cycom may increase the Software License Fee for CityLaw Software by no more than five percent (5%) per year. Not less than thirty (30) days prior to the expiration of the SOW Initial Term or any subsequent SOW Renewal Term, Cycom shall give the Municipality written notice of Cycom's access and use Fee for CityLaw Software for the next year. Such notice may be provided to

3. Changing Number of Users

The Municipality may add or remove licensed Users for the CityLaw Software license; provided, however,
that the Municipality shall pay Cycom the monthly license Fee for each licensed User that is licensed to use the CityLaw Software corresponding to such license during the applicable monthly billing period, regardless of when the User becomes licensed within that monthly billing period.

4. System

The System shall be provided by the Municipality (whether as property owned by the Municipality or as
property provided to the Municipality by one or more third parties in an arrangement not involving Cycom), and not by Cycom.

5. Fee—Description

The Fee for the CityLaw Software Services shall include: (i) the license Fee for the CityLaw Software, (ii)
all initial installation, custom installation, and training for the CityLaw Software prior to Acceptance (as defined below) of the CityLaw Software. Receipt of Software maintenance releases, updates and improvements shall be subject to payment of the Fee for support and maintenance Services as defined in Exhibit A-9 ("Support and Maintenance Rider").

6. Free Live Remote Training

The Municipality's purchase of the CityLaw Software Services from Cycom shall include eight (8) hours oflive remote training, designed to supplement Cycom's free on-demand video training course available in Cycom's online Help Center at https://cycom.zendesk.com/hc. Cycom does not place a limit on the number of attendees for a remote training session. Notwithstanding the foregoing, Cycom reserves the right to modify the availability of, and any or all terms and conditions of, such live remote training.

Acceptance of Software

1. Acceptance Definition. "Acceptance" means the process of approval and acceptance, by the Municipality, of the installation and initial setup and configuration of the Software, or of any module of the Software, on the System, by Cycom.

2. Acceptance Triggers Payment Schedules. Acceptance of the Software shall be the triggering event for the first payment of: (i) the payment schedule for the CityLaw Software Services listed above, and (ii) the payment schedule for the support and maintenance Services payment schedule listed in Exhibit A-9 ("Support and Maintenance Rider").

3. Acceptance Procedure. The Municipality shall have thirty (30) days from completion of the installation and initial setup and configuration of the Software, or of any module of the Software, to test whether the Software, or such module of the Software, materially conforms to the operational, functional and performance specifications represented by Cycom. Failure of the Municipality to notify Cycom in writing, in conformity with the provisions of Section 24.1 ("Notices") of the MSA, within such testing period, that the Software, or such module of the Software, fails to materially conform to the specified performance standards shall be deemed to constitute "Acceptance" of the Software, or of such module of the Software.

Exhibit A-9

This Support and Maintenance Rider ("Exhibit A-9") is entered into, to be effective as of the SOW Effective Date (as defined in the SOW), by and between Cycom and the Municipality, and specifies certain of the particular
Services, including activities and deliverables, described in more detail below, to be performed hereunder by
Cycom for the Municipality.

1. Incorporation into SOW

This Exhibit A-9 shall be incorporated into and made a part of and governed by the terms of that certain Statement of Work, effective as of the Effective Date stated therein, entered into by and between the Municipality and Cycom, and as amended (the "SOW"). Capitalized terms used, but not otherwise defined, in this Exhibit A-9 shall have the meanings ascribed to them in the SOW or the MSA.

2. Service Details and Fees

Cycom shall provide support and maintenance Services to the Municipality with respect to the use and maintenance of the Software, including maintaining proper performance of the Software, installing software updates and new versions of the Software, maintaining network connections to the Software, supporting interface of the Software with certain third-party software (to the extent that the Municipality has purchased
support for such interface), troubleshooting, supporting the Municipality's authorized Users, and supporting the
Municipality's IT department. Support and maintenance Services include: (i) an online knowledge base available on Cycom's website at https://cycom.zendesk.com/hc/en-us or a successor website address, (ii) email support, and (iii) phone support. The following terms shall govern the Services provided under this Exhibit A-9:

Term of Support and Maintenance Services	Beginning on the Effective Date and ending Twelve (12) Months after.
Limitations on Fee Increase	Cycom may increase the Fee for support and maintenance Services by no more than three percent (3%) per year. Not less than sixty (60) days prior to the expiration of the SOW Initial Term or any subsequent SOW Renewal Term, Cycom shall give the Municipality written notice of Cycom's Fee for support and maintenance Services for the next year. Such notice may be provided to the Municipality in the form of an invoice.

Renewal of Term of Support and Maintenance Services	In order to renew support and maintenance Services for any period beyond the expiration of the SOW Initial Term or any subsequent SOW Renewal Term, the Municipality must execute a written document that satisfies the Municipality's internal procurement and contracting policies. If the Municipality, for any reason whatsoever, chooses to terminate support and maintenance Services after the expiration date of the SOW Initial Term or any subsequent SOW Renewal Term, it shall deliver a notice of non- renewal to Cycom at least thirty (30) days prior to such expiration date. If Cycom, for any reason whatsoever, chooses not to provide support and maintenance Services after the expiration date of the SOW Initial Term or any subsequent SOW Renewal Term, it shall deliver a notice of non-renewal to the Municipality not less than sixty (60) days prior to such expiration date. If the Municipality, for any reason whatsoever, chooses to terminate support and maintenance Services at the end of any billing period prior to the expiration date of the SOW Initial Term or any subsequent SOW Renewal Term, it shall deliver a notice of termination of such Services to Cycom at least ten (10) days prior to the end of such billing period. If Cycom, for any reason whatsoever, chooses not to provide support and maintenance Services at the end of any billing period prior to the expiration date of the SOW Initial Term or any subsequent SOW Renewal Term, it shall deliver a notice of termination of such Services to the Municipality not less than thirty (30) days prior to the end of such billing period. Notwithstanding the foregoing, Cycom shall not exercise such right of termination at a time that causes the termination to be effective any earlier than three (3) months following the SOW Effective Date.

3. Changing Number of Users

The Municipality may add or remove licensed Users for the support and maintenance Services; provided,
however, that the Municipality shall pay Cycom the monthly Fee for each authorized User during the applicable monthly billing period, regardless of when the User becomes licensed within that monthly billing period.

4. Out of Scope Work

The Services do not include service to facilities outside of the System, assistance moving the Municipality's operations or equipment from the Municipality's premises located at 415 Diamond Street, Redondo Beach, CA 90277 (the "Premises"), or significant reconstructive work following flood, fire, theft, or any other extraordinary event, all of which shall be billed separately pursuant to mutually agreeable terms. Any migration/upgrade projects that require advanced planning and support shall be scoped and billed outside of this Exhibit A-9.

5. Support Ticket Procedure

Users may call Cycom's telephone support line at 888-292-6688, which is staffed between 7:00 AM and 7:30 PM CDT. If no one is available to take the call, or if the call is received outside of those hours, it will go to voicemail and a support ticket will be created automatically. Users may also contact the Cycom Support Team via email at support@cycominc.com. Any email sent to this address will create a support ticket. Once a Support Ticket is created, work shall be prioritized by issue severity and then by date and time.

1. Responsibility of Municipality's IT Department for Certain Issues. If the Cycom Support Team determines that an issue is outside the scope of Cycom's products and services, the Support Team shall communicate such determination to the ticket requester and shall advise the ticket requester to contact the Municipality's Primary IT Contact.

2. Issues Outside the Scope of Support Team Expertise. If the Cycom Support Team determines that an issue is related to the installation of the Software, the issue shall be escalated to the Cycom

Maintenance Team. If the Maintenance Team determines that the issue is caused by a defect in the Software (e.g. a software bug), the issue shall be escalated to the Cycom Development Team. Both the Maintenance Team and the Development Team shall work directly with the Support Team to resolve the issue. Throughout the entire process, the Support Team shall update the ticket requester, or the appropriate Municipality contact person, on the progress toward resolution.

6. Support and Maintenance Services—In General

1. Conformity. Within a reasonable time, Cycom will provide such assistance as is necessary to cause the Software to perform in accordance with the Documentation.

2. Improvements. Within a reasonable time, Cycom will provide such improvements, enhancements, and other changes to the Software suitable to the uses made of the Software by the Municipality, and will make known to the Municipality any improvements as they are developed.

3. New Operating System; Server-side Maintenance. Within a reasonable time, Cycom will provide updates to the Software if and as required to cause it to operate under new releases of the operating system so long as such updates are technically feasible. Server-side maintenance of the Software, such as updates and upgrades, will be performed at no additional fee Monday through Friday between the hours of 7:00am and 4:00pm Central Daylight Time. Server-side maintenance of the Software outside of these hours can be scheduled with Cycom for an additional fee.

4. Hours. Cycom will provide customer support Monday through Friday between the hours of 7:00am to 7:00pm Central Daylight Time. This does not include server-side maintenance to the Software, such as updates and upgrades.

5. Initial Response Time. Support service will provide a response less than two (2) hours from time of message receipt. Support issues are prioritized by issue severity then receipt order.

6. Remote Sessions. Cycom will be provided with telecommunication access for support, which shall be used on an as-needed basis and with notification given to the Municipality before a remote support session is begun.

7. Software Error Severity Classifications and Support Request Resolution Process

1. Error—Definition. "Error" means any reported malfunction, error or other defect in the Software that can be reproduced by Cycom and that constitutes a non-conformity from the Documentation. Each Error will be assigned a severity level as further detailed in Section 6.2 ("Software Error Severity Classifications"), below.

2. Software Error Severity Classifications. All Software Errors shall be classified by Cycom as follows:

Error Severity Level	Definition	Examples
1 ("S1")	Urgent: Severe problem preventing User or workgroup from performing critical business functions	- Software data corruption (data loss, data unavailable). - Software crash or hang where no workaround exists. - Software significantly impacted, such as severe performance degradation. - Software and/or data is at high risk of potential loss or interruption. - Software workaround is required immediately. - Time-critical Software cutover impacted.
2 ("S2")	High: User or workgroup able to perform job function, but performance of job function degraded or severely limited	- Software adversely impacted. - Non-Software data corruption (data loss, data unavailable). - Non-Software crash or hang. - Non-Software and/or data is at high risk of potential loss or interruption. - Non-Software workaround is required immediately.
3 ("S3")	Medium: User or workgroup performance of job function is largely unaffected	- Software has encountered a non-critical problem or defect and/or questions have arisen on product use.

4 ("S4")	Low: Minimal system impact; includes feature requests and other non- critical questions	- No Municipality business impact. - Requests for enhancements by Municipality.

3. Software Support Service Level Objectives (SLOs). Cycom will use reasonable commercial efforts to provide the Municipality with technical advice and assistance in connection with the Municipality's use of the Software according to Severity Level. The table below sets forth Cycom's targets for support responses to Software Errors based on Severity Level:

Severity Level	Initial Target Response	Target Work Effort	Target Communication Frequency
S1	2 hours (7:00 AM - 7:30 PM CDT)	Continuous during business hours (7:00 AM - 7:30 PM CDT) until solution to problem is identified.	Once per day (business day only).
S2	4 hours (7:00 AM - 7:30 PM CDT)	Daily, during Municipality business hours only.	Once every 2-3 days (business day only).
S3	8 hours (7:00 AM - 7:30 PM CDT)	Weekly during business hours.	Once a week.
S4	12 hours (7:00 AM - 7:30 PM CDT)	Every other week during business hours.	Once a month.

4. Software Support Request Resolution Process.

   a. Process. Cycom handles all Municipality support requests on a first-in-first-out basis. Cycom shall prioritize all Errors according to their impact to the Municipality using the severity definitions described in Section 6.2 ("Software Error Severity Classifications"), above. Cycom may upgrade or downgrade the severity of an Error depending on developments during the resolution process. For example, if available, a temporary resolution may be provided to mitigate the material impact of a given Error, resulting in the reduction of the Severity Level.

   b. Escalation. If the Municipality and Cycom are unable to mutually agree upon a resolution plan

for S1 and S2 Errors, then the Parties shall escalate the support request in accordance with Cycom's escalation process. Once the escalation process has been initiated, Cycom shall provide the Municipality with
support request progress updates via phone or email on a mutually agreed-upon schedule. Such progress
updates shall include information about the Error description, daily progress, root cause (if known) and overall plan to resolve the Error.

8. Exclusions

1. Use. The Services specifically exclude support for any Errors caused by (i) access to or use of the Software or the System in any manner other than that for which the Software is licensed or for which the right to access and use the System is given; (ii) any installation, integration, modification, or repair of the Software made by any person other than Cycom; (iii) installation in the System of any hardware, software or firmware that is specifically disapproved by Cycom; (iv) unusual physical, electrical or electromagnetic stress, fluctuations in electrical power beyond System hardware specifications, or failure of air conditioning or humidity control; and (v) the Municipality's accident, misuse, or neglect, or causes not attributable to normal wear and tear. In addition, support excludes any Errors for which a correction is available in a subsequent Software release other than that currently operated by the Municipality and which has been made available to the Municipality by Cycom.

2. Supported Versions. The Services also specifically exclude support for any version of the Software, or of other software released by any third-party software vendor, which has reached its "end of primary support" (EOPS) date, as determined by Cycom. In order to continue to receive ongoing support Services hereunder for any software release which is beyond its EOPS date, the Municipality must upgrade to a currently supported software release. Notwithstanding the foregoing, the time period for continuing support Services hereunder for any such software release which is beyond its EOPS date may be extended by Cycom in its sole discretion.

9. Reinstatement of Lapsed Support

If the support and maintenance Services expire or are terminated due to the Municipality's failure to pay support and maintenance Services Fees, and the Municipality subsequently seeks to reinstate support and maintenance Services, the Municipality shall pay: (a) the cumulative support and maintenance Services Fees applicable for the period during which support and maintenance Services lapsed; (b) the support and maintenance Services Fees for the current period during which the Municipality has subscribed for support and maintenance Services; and (c) the then-current reinstatement Fee, as quoted by Cycom.

Exhibit B

Acceptable Use Policy

SOC 2 Criteria: CC1.1, CC1.4, CC1.5, CC2.2, CC5.2

Keywords: Background Checks, Security Awareness Training, Hard Drive Encryption, Anti-Virus Software

---

Background

Cycom Data Systems is committed to ensuring all workforce members actively address security and compliance in their roles at Cycom Data Systems. We encourage self-management and reward the right behaviors.

Purpose

This policy specifies acceptable use of end-user computing devices and technology. Additionally, training is imperative to assuring an understanding of current best practices, the different types and sensitivities of data, and the sanctions associated with non-compliance.

Policy

Cycom Data Systems policy requires all workforce members to accept and comply with the Acceptable Use Policy. Cycom Data Systems policy requires that:

- Background verification checks on all candidates for employees and contractors should be carried out in accordance with relevant laws, regulations, and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risk.
- Employees, contractors and third party users must agree and sign the terms and conditions of their employment contract, and comply with acceptable use.
- Employees will go through an onboarding process that familiarizes them with the environments, systems, security requirements, and procedures Cycom Data Systems has in place. Employees will also have ongoing security awareness training that is audited.
- Employee offboarding will include reiterating any duties and responsibilities still valid after terminations, verifying that access to any Cycom Data Systems systems has been removed, as well as ensuring that all company owned assets are returned.
- Cycom Data Systems and its employees will take reasonable measures to ensure no corporate data is transmitted via digital communications such as email or posted on social media outlets.
- Cycom Data Systems will maintain a list of prohibited activities that will be part of onboarding procedures and have training available if/when the list of those activities changes.
- A fair disciplinary process will be utilized for employees that are suspected of committing breaches of security. Multiple factors will be considered when deciding the response, such as whether or not this was a first offense, training, business contracts, etc. Cycom Data Systems reserves the right to terminate employees in the case of serious cases of misconduct.

Procedures

Cycom Data Systems requires all workforce members to comply with the following acceptable use requirements and procedures, such that:

- All workforce members are primarily considered as remote users and therefore must follow all system access controls and procedures for remote access.
- Use of Cycom Data Systems computing systems is subject to monitoring by Cycom Data Systems IT and/or Security team.
- Employees may not leave computing devices (including laptops and smart devices) used for business purposes, including company-provided and BYOD devices, unattended in public.
- Device encryption must be enabled for all mobile devices accessing company data, such as whole-disk encryption for all laptops.
- Use only legal, approved software with a valid license installed through a pre-approved application store. Do not use personal software for business purposes and vice versa.
- Encrypt all email messages containing sensitive or confidential data.
- Employees may not post any sensitive or confidential data in public forums or chat rooms. If a posting is needed to obtain technical support, data must be sanitized to remove any sensitive or confidential information prior to posting.
- Anti-malware or equivalent protection and monitoring must be installed and enabled on all endpoint systems that may be affected by malware, including workstations, laptops and servers.
- All data storage devices and media must be managed according to the Cycom Data Systems Data Classification specifications and Data Handling procedures.

Asset Management Policy

SOC 2 Criteria: CC2.1, CC6.1

Keywords: Asset Inventory, Anti-Virus, Network Diagram, Hardening Standards

---

Purpose

The purpose of this policy is to define requirements for tracking Cycom Data Systems logical and physical assets through their lifecycle from initial acquisition to final disposal. This policy supports the Data Classification Policy which establishes a framework for classifying corporate and customer data based on its level of sensitivity, value, and criticality to Cycom Data Systems.

Physical and Virtual Asset Standard

An inventory process must be in place to support the discovery, management and replacement/disposal of all significant physical and virtual assets. The inventory process should facilitate the identification and removal of any illegal or unauthorized software found in the Cycom Data Systems environment. The inventory process must include the following:

- A listing that captures appropriate details of significant Information and technology assets under Cycom Data Systems management or control, including physical and virtual assets.
    - Details should include a description of the type of asset, the make of the asset, technical specifications, license details, and versions of the software packages or operating systems.
- Items can be excluded from the inventory if they carry very low purchase/replacement costs (including time and labor needed to install and configure) and pose little or no risk to business operations or compliance status.
- Each significant asset is associated with an identifier, license, or tag so that it can be identified and tracked.
- Whether through depreciation, expiring leases or agreements, obsolescence/end of support, loss, or other reasons, the disposal/replacement of physical and virtual assets must be tracked.
- A reporting function must support auditing and monitoring for IT compliance with this standard.

Asset Inventory Standard

An asset inventory process must be in place to support the technological management of critical business processes and to meet legal and regulatory requirements. Cycom Data Systems collects and stores the necessary information for the asset inventory which includes:

- A unique identifier or name of the asset.
- The owner of the system – typically, but not necessarily the information resource owner.
- A description of the purpose of the asset and the role the asset has in supporting critical business processes and in meeting legal or regulatory requirements.

Physical Asset Inventory

Cycom Data Systems leverages a SaaS-based asset management system, Drata, to maintain inventory of all company owned physical computing equipment, including but not limited to:

- Servers
- Workstations
- Laptops
- Printers
- Networking equipment

All company-owned devices are subject to a complete data wipe if deemed necessary, such as in the case of device infection or repurpose. This data wipe will be carried out by the IT manager.

Digital Asset Inventory

Cycom Data Systems uses Drata’s automated system to query across our cloud-based infrastructure to obtain detailed records of all digital assets, including but not limited to:

- Virtual machines
- Virtual servers
- Virtual repositories
- Security agents

- Source code repositories
- User accounts

The records are stored in a database system maintained by Cycom Data Systems. Records are tagged with owner/project and classification when applicable. All records are kept up to date through automation via Drata.

System Retirement Standard

The information resource owner determines when a system no longer is needed or is obsolete and can be retired. If the system to be replaced/retired supports mandatory legal and regulatory requirements of critical business processes, the information resource owner must ensure that any replacement system can support these processes before the current system is retired.

Before retiring/replacing any system, data retention requirements for all data stored or managed by that system must be reviewed, and a plan for complying with all applicable data retention requirements must be developed and executed. This is particularly important for systems that manage data subject to legal/regulatory scrutiny. Any data subject to data retention requirements must be migrated to an appropriate destination and tested for appropriateness, completeness, accessibility and retrievability from the destination before the original data is deleted from the original system as part of the system retirement process.

System Hardening Standards

Device Best Practices and Hardening Standards

- Manufacturer-provided hardening and best practice guides will be employed to ensure all device installation is properly guarded from vulnerabilities and unauthorized attempts to access the systems.
    - Center for Internet Security (CIS) benchmarks are utilized where possible for system hardening guidance. (https://www.cisecurity.org/cis-benchmarks/)
- Vendor supplied defaults, including usernames, passwords, and any other common settings that may result in unauthorized attempts to access the systems, will be changed in accordance with hardening guides.
- Insecure and unnecessary communication protocols are disabled.
- Local passwords, when required, will be randomly generated and securely stored in the approved password management system.
- Current patches will be installed.
- Malware protection will be implemented.
- Logging will be enabled.
- Two-factor authentication should be used whenever available/supported on the device platform.

Infrastructure Configuration and Maintenance

- Internal Workstation and Server Patching
    - Operating system patches/upgrades are evaluated periodically.
    - Operating system and security patches/upgrades are installed based on their criticality.
    - Operating system patches/upgrades are installed during off-peak hours to minimize the disruption to business processes.
- Internal Infrastructure Patching
    - Infrastructure (routers, switches, virtual hosts, etc.) patches/upgrades are evaluated as they come available from vendors.
    - Infrastructure patches/upgrades are installed based on their criticality.
    - Infrastructure patches/upgrades are reviewed and approved via a lab environment when possible/practical.
    - Infrastructure patches/upgrades are installed during off-peak hours to minimize the disruption to business processes.
    - When applicable, redundant systems are patched/upgraded one device at a time to ensure no impact to shared services.
    - Networking hardware/software updates follow the regular change management procedures.
- Infrastructure Support Documentation
    - A network diagram is available to all appropriate service personnel and is kept current.
    - Configuration standards for the setup of all infrastructure devices are in place and are formally documented as necessary.
- Endpoint Security/Threat detection
    - Controls are in place to restrict the use of removable media to authorized personnel
    - Antivirus and anti-malware tools are deployed on end-point devices (e.g., workstations, laptops, and mobile devices).
    - Antivirus and anti-malware tools are configured to automatically receive updates, run scans and alert appropriate personnel of viruses or malware.

Backup Policy

SOC 2 Criteria: CC9.1, A1.2

Keywords: Multiple availability zones, Backup frequency

Purpose

To protect the confidentiality, integrity, and availability of data, both for Cycom Data Systems and Cycom Data Systems's customers, complete backups are performed daily to assure that data remains available when it's needed and in the case of a disaster.

Policy Statements

Cycom Data Systems policy requires that:

- Data should be classified at time of creation or acquisition according to the Data Classification Policy
- An up-to-date inventory and data flow map of all critical data are maintained.
- All business data should be stored or replicated into a company controlled repository, including data on end-user computing systems.
- Data must be backed up according to its level defined in Data Classification Policy.
- Data retention period must be defined and comply with any and all applicable regulatory and contractual requirements. More specifically,
    - Data and records belonging to Cycom Data Systems customers must be retained per Cycom Data Systems product terms and conditions and/or specific contractual agreements.
    - By default, all security documentation and audit trails are kept for a minimum of seven years, unless otherwise specified by Cycom Data Systems's Data Classification Policy, specific regulations, or contractual agreement.

Backup and Recovery

Customer Data

Cycom Data Systems stores customer data in a secure production account in Azure, using Azure SQL databases. By default, Azure SQL provides durable infrastructure to store important data and is designed for durability of 99.999999999% of objects.

Cycom Data Systems performs automatic backups of all customer and system data to protect against catastrophic loss due to unforeseen events that impact the entire system. An automated process will back up all data to a separate region in the same country (e.g. US East to US West). By default, data will be backed up daily. The backups are encrypted in the same way as live production data. Backups are monitored and alerted by Azure Monitor. Backup failures trigger an incident by alerting the Security Officer.

Source Code

Cycom Data Systems stores its source code in git repositories hosted by Azure DevOps. Source code repositories are backed up to Cycom Data Systems's Azure account on a weekly basis. In the event that **Azure DevOps** suffers a catastrophic loss of data, source code will be restored from the backups in Azure.

Business Continuity Plan

SOC 2 Criteria: CC5.3, CC7.5

Keywords: Status Page, Worksite Recovery

Purpose

This policy establishes procedures to recover Cycom Data Systems following a disruption. This Policy is maintained by the Cycom Data Systems Security Officer and Privacy Officer.

Policy

Cycom Data Systems policy requires that:

- A plan and process for business continuity, including the backup and recovery of systems and data, must be defined and documented.
- The Business Continuity Plan shall be simulated and tested at least once a year. Metrics shall be measured and identified recovery enhancements shall be filed to improve the process.
- Security controls and requirements must be maintained during all Business Continuity Plan activities.

Line of Succession

The following order of succession ensures that decision-making authority for the Cycom Data Systems Business Continuity Plan is uninterrupted. The CEO is responsible for ensuring the safety of personnel and the execution of procedures documented within this Plan. The Head of Engineering is responsible for the recovery of Cycom Data Systems technical environments. If the CEO or Head of Engineering is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the Business Operations Lead shall function as that authority or choose an alternative delegate.

Response Teams and Responsibilities

The following teams have been developed and trained to respond to a contingency event affecting Cycom Data Systems infrastructure and systems.

1. HR & Facilities is responsible for ensuring the physical safety of all Cycom Data Systems personnel and environmental safety at each Cycom Data Systems physical location. The team members also include site leads at each Cycom Data Systems work site. The team leader is the Head of HR who reports to the CEO.
2. DevOps is responsible for assuring all applications, web services, platforms, and their supporting infrastructure in the Cloud. The team is also responsible for testing re-deployments and assessing damage to the environment. The team leader is the Head of Engineering.
3. Security is responsible for assessing and responding to all cybersecurity related incidents according to Cycom Data Systems Incident Response policy and procedures. The security team shall assist the above teams in recovery as needed in non-cybersecurity events. The team leader is the Security Officer.

Members of above teams must maintain local copies of the contact information of the Business Continuity Plan succession team. Additionally, the team leads must maintain a local copy of this policy in the event Internet access is not available during a disaster scenario.

All executive leadership shall be informed of any and all contingency events.

Work Site Recovery

In the event a Cycom Data Systems facility is not functioning due to a disaster, employees will work from home or locate to a secondary site with Internet access, until the physical recovery of the facility impacted is complete.

Cycom Data Systems's software development organization has the ability to work from any location with Internet access and does not require an office provided Internet connection.

Application Service Event Recovery

Cycom Data Systems maintains a status page to provide real time updates and inform customers of the status of each service. The status page is updated with details about an event that may cause service interruption / downtime. Cycom Data Systems's status page:

https://status.cycominc.com

Code of Conduct

SOC 2 Criteria: CC1.1, CC1.4, CC1.5, CC2.2, CC5.3

Keywords: Ethical Behavior, Safety, Harassment, Disciplinary Action, Law Enforcement

---

Purpose

The Cycom Data Systems Code of Conduct ("Code") is built around our belief that everything we do will be measured against the highest possible standards of ethical business conduct. Our commitment to high standards helps us hire great people, build great products, and attract loyal customers.

Who must follow the Code?

We expect all employees to know and follow the Code. Failure to do so can result in disciplinary action, up to and including termination of employment. We also expect our contractors, consultants, and others who may be temporarily assigned to perform work or services for Cycom Data Systems to follow the Code when they work with us. Failure of a Cycom Data Systems contractor, consultant, or other service provider to follow the Code can result in termination of their relationship with Cycom Data Systems.

Who to ask about the Code?

If you have a question or concern about the Code, be proactive and contact your manager. You can also submit a question or raise a concern regarding a suspected violation of our Code (or any other Cycom Data Systems policy) to your manager.

No Retaliation

Cycom Data Systems prohibits retaliation against anyone who reports, or participates in an investigation of, a possible violation of our Code, our policies, or the law. Please contact a member of senior management if you believe that you are the subject of retaliation within Cycom Data Systems.

Code of Conduct

As a Cycom Data Systems employee, you're expected to be honest, act ethically, and demonstrate integrity in all situations. You have a duty to follow policies and procedures found in this Code of Conduct, as well as those that are specific to your job. You must also comply with all laws that apply to our business. Most of the time, common sense and good judgment provide excellent guideposts. If you're unsure about the right thing to do, ask someone on the management team.

Before you act, ask yourself:

- Is this the right thing to do?
- Is it legal?
- Do I have the authority to act?
- Does the action comply with the Code of Conduct and policies and procedures?
- If this action became public, how would it look in the news media?
- Would I be upset or embarrassed if other people found out about this action?

If your answer to any of these questions raises doubts, talk with your supervisor, anyone in management, or the Cycom Data Systems Compliance Officer. If you're a supervisor or a manager, you're responsible for knowing the rules and reviewing the Code of Conduct with the people who report to you to make sure they're familiar with its contents. You're also responsible for preventing violations of the Code, as well as detecting violations that may occur and reporting them appropriately.

You're expected to:

- Lead with integrity.
- Encourage employees to ask questions and expand their knowledge of the rules.
- Demonstrate integrity by acting promptly and effectively when necessary.
- Educate employees on compliance policies specific to their job responsibilities.

Quality Work Environment

We are committed to a supportive work environment, where our employees have the opportunity to reach their fullest potential. Members of our Cycom Data Systems team are expected to do their utmost to create a workplace culture that is free of harassment, intimidation, bias, and unlawful discrimination. Please read the Employee Handbook for greater detail about how we should conduct ourselves at work.

1. **Equal opportunity employment**

Employment at Cycom Data Systems is based solely upon individual merit and qualifications directly related to professional competence. We strictly prohibit unlawful discrimination or harassment on the basis of race, color, religion, veteran status, national origin, ancestry, pregnancy

status, sex, gender identity or expression, age, marital status, mental or physical disability, medical condition, sexual orientation, or any other characteristics protected by law. We also make reasonable accommodations to meet our obligations under laws protecting the rights of the disabled.

1. **Harassment, discrimination, and bullying**

Cycom Data Systems strictly prohibits discrimination, harassment, and bullying in any form – verbal, physical, or visual. If you believe that you've been bullied or harassed by anyone at Cycom Data Systems, or anyone connected to Cycom Data Systems (such as a partner or vendor), please immediately report the incident to your manager or the HR team. HR will promptly and thoroughly investigate any complaints and take appropriate action.

1. **Drugs and alcohol**

Substance abuse is incompatible with the health and safety of our employees, and we don't permit it. Consumption of alcohol is allowed at our office on special occasions, but we ask everyone to use good judgment and never drink in a way that: (i) leads to impaired performance or inappropriate behavior, (ii) endangers the safety of others, or (iii) violates the law. Illegal drugs in our offices or at work-related events are strictly prohibited.

1. **Safe workplace**

We are committed to a violence-free work environment. We will not tolerate any level of violence or the threat of violence in the workplace. No one should bring a weapon to work under any circumstances. If you become aware of a violation of this policy, report it to a member of senior management immediately.

Avoid conflicts of interest

As Cycom Data Systems employees, we should avoid conflicts of interest and circumstances that reasonably present the appearance of a conflict of interest, especially if it would create an incentive for you or present the appearance of an incentive for you, (whether directly or indirectly).

Here is list of areas where conflicts of interest often arise:

- Personal investments (e.g. with competitors)
- Outside employment, advisory roles, and board seats
- Business opportunities found through your work at Cycom Data Systems
- Inventions influenced by your work at Cycom Data Systems
- Business opportunities involving friends and relatives
- Acceptance of gifts, entertainment, and other business courtesies

If you are unsure if there is a conflict of interest, contact the Compliance or Legal teams to

discuss.

Preserve confidentiality

Throughout its lifecycle, all nonpublic information that is processed, transmitted, and/ or stored

by Cycom Data Systems must be protected in a manner that is consistent with our contractual and legal requirements and reasonable and appropriate for the level of sensitivity, value, and risk associated with *Nonpublic* information (please see the Data Classification Policy). Information that contains data elements from multiple classifications must be protected at the highest level of information represented. For example, a document that contains *Nonpublic* and *Public* information must be treated as *Nonpublic* information. Nonpublic information must be secured against disclosure, modification, and access by unauthorized individuals. Therefore, the information must be:

- Secured at rest; and
- Secured in transit; and
- Securely destroyed in accordance with record retention policies and procedures.

Information Security

You're responsible for using Cycom Data Systems's computer resources properly – especially with regard to information security – and you need to be thoroughly familiar with Cycom Data Systems's Information Security policies and procedures.

These steps can go a long way in preventing unauthorized access:

- Never share your login information.
- Lock your workstation when you step away.
- Log off your workstation when you leave for the day.
- Clear your workstation, waste can, printers and fax machines of sensitive information, such as PII or company-sensitive information.

Protect Cycom Data Systems's Assets

1. **Intellectual property**

Cycom Data Systems's intellectual property rights (e.g. patents, trademarks, copyrights, trade secrets, and "know-how") are valuable assets. Unauthorized use can lead to their loss or serious loss of value. You must comply with all intellectual property laws, including laws governing the fair use of copyrights and trademarks. You must never use Cycom Data Systems's trademarks or other protected information or property for any business or commercial venture without pre-clearance from the Marketing team. Report any suspected misuse of trademarks or other Cycom Data Systems intellectual property to the Legal or compliance team.

Likewise, respect the intellectual property rights of others. Inappropriate use of others'

intellectual property may expose Cycom Data Systems and you to criminal and civil fines and penalties. Seek advice from the Legal team before you solicit, accept, or use proprietary information from individuals outside the company or allow them obtain access to Cycom Data Systems proprietary information. You should also check with the Legal team if developing a product feature that uses content not belonging to Cycom Data Systems.

1. **Company Equipment**

Cycom Data Systems gives us the tools and equipment that we need to do our jobs effectively, but counts on us to be responsible and not wasteful. Uncertain whether personal use of company assets is okay? Ask your manager.

1. **The Network**

Cycom Data Systems's network, software, and computing hardware are a critical aspect of our company's physical property and intellectual property. Follow all security policies diligently. If you have any reason to believe that our network security has been violated – for example, you lose your laptop or think that your network password may have been compromised – promptly report the incident to your manager.

1. **Physical Security**

Bad actors may steal company assets. Always secure your laptop, important equipment, and your personal belongings, even while on company premises. Promptly report any suspicious activity to your manager.

Ensure financial integrity and responsibility

Financial integrity and fiscal responsibility are core aspects of corporate professionalism. Each

person at Cycom Data Systems has a role in making sure that money is appropriately spent, our financial records are complete and accurate, and internal controls are honored. This is applicable every time that we hire a new vendor, expense something to Cycom Data Systems, or sign a new business contract.

It's important that we also keep records for an appropriate length of time. Cycom Data Systems's Data Retention Policy suggests minimum record retention periods for certain types of records. These guidelines help keep in mind applicable legal requirements, accounting rules, and other external requirements. Contractual obligations may sometimes specify longer retention periods for certain types of records. In addition, if you are asked by the Legal team to retain records relevant to a litigation, audit, or investigation, do so until Legal tells you that retention is no longer necessary. If you have any questions regarding the correct length of time to retain a record, contact the Compliance or Legal teams.

Obey the law

Cycom Data Systems takes its responsibilities to comply with laws very seriously. Every employee is expected to comply with applicable legal requirements and restrictions. You should understand the laws and regulations that apply to your work. Contact the Compliance or Legal teams if you have any questions.

Policy Compliance

Compliance Measurement

The Compliance team will verify compliance with this Code through various methods (e.g.

periodic manager reviews, tool reports, internal and external audits, and employee feedback).

Exceptions

Any exception to this Code must be approved by the Compliance team in writing.

Non-Compliance

Any employee who violates this Code may be subject to disciplinary action, up to and including

termination of employment in addition to any civil and criminal liability.

Your Annual Acknowledgment of the Code of Conduct

Once each year, as a condition of your employment, you're required to acknowledge that you have received the Code of Conduct and understand its rules. New employees will sign an acknowledgment when they start with the company. Basically, your annual acknowledgment confirms that:

- You've reviewed the Code of Conduct and you are required to comply with the Code of Conduct; you will comply with the compliance policies and procedures, as well as policies and procedures related to your job responsibilities;
- You will report any questions or concerns about suspected or actual violations of the Code to your supervisor, anyone in management or Cycom Data Systems's Compliance Officer,
- To the best of your knowledge, you haven't acted contrary to the Code of Conduct
- You have reported any potential conflicts of interest to the Compliance Department.

Data Classification Policy

SOC 2 Criteria: C1.1, PI1.1

Keywords: Confidential Data, Internal Data, Public Information, Restricted Data

---

Purpose

This policy will assist employees and other third-parties with understanding the Company's information labeling and handling guidelines. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect sensitive or confidential information (e.g., Company Confidential information should not be left unattended in conference rooms).

Scope

Information covered in this policy includes, but is not limited to, information that is received, stored, processed, or transmitted via any means. This includes electronic, hardcopy, and any other form of information regardless of the media on which it resides.

Policy

Definitions

- **Confidential/Restricted Data**:

Generalized terms that typically represent data classified as *Sensitive or Private*, according to the data classification scheme defined in this policy.

- **Internal Data**:

All data owned or licensed by Cycom Data Systems.

- **Public Information**:

Any information that is available within the public domain.

Data Classification Scheme

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to Cycom Data Systems should that data be disclosed, altered, or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All data should be classified into one of the three following classifications.

Confidential/Restricted Data

Data should be classified as Restricted or Confidential when the unauthorized disclosure, alteration, or destruction of that data could cause a significant level of risk to Cycom Data Systems or its customers. Examples of Sensitive data include data protected by state or federal privacy regulations (e.g. PHI & PII) and data protected by confidentiality agreements. The highest level of security controls should be applied to Restricted and Confidential Data:

- Disclosure or access to Restricted and Confidential data is limited to specific use by individuals with a legitimate need-to-know. Explicit authorization by the Security Officer is required for access to because of legal, contractual, privacy, or other constraints.
- Must be protected to prevent loss, theft, unauthorized access, and/or unauthorized disclosure.
- Must be destroyed when no longer needed. Destruction must be in accordance with Company policies and procedures.
- Will require specific methodologies, procedures, and reporting requirements for the response and handling of incidents.

Internal Use Data

Data should be classified as Internal Use when the unauthorized disclosure, alteration, or destruction of that data could result in a moderate level of risk to Cycom Data Systems or its customers. This includes proprietary, ethical, or privacy considerations. Data must be protected from unauthorized access, modification, transmission, storage or other use. This applies even though there may not be a civil statute requiring this protection. Internal Use Data is restricted to personnel who have a legitimate reason to access it. By default, all data that is not explicitly classified as Restricted/Confidential or Public data should be treated as Internal Use data. A reasonable level of security controls should be applied to Internal Use Data.

Public Data

Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to Cycom Data Systems and its customers. It is further defined as information with no existing local, national, or international legal restrictions on access or usage. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized alteration or destruction of Public Data.

Calculating Classification

The goal of information security, as stated in the Information Security Policy, is to protect the confidentiality, integrity, and availability of Corporate and Customer Data. Data classification reflects the level of impact to Cycom Data Systems if confidentiality, integrity, or availability is compromised. If a classification is not inherently obvious, consider each security objective using the following table as a guide. All data are to be assigned one of the following four sensitivity levels:

CLASSIFICATION	DATA CLASSIFICATION DESCRIPTION	
RESTRICTED	Definition	Restricted information is highly valuable, highly sensitive business information and the level of protection is dictated externally by legal and/or contractual requirements. Restricted information must be limited to only authorized employees, contractors, and business partners with a specific business need.
	Potential Impact of Loss	**SIGNIFICANT DAMAGE** would occur if Restricted information were to become available to unauthorized parties either internal or external to Cycom Data Systems. Impact could include negatively affecting Cycom Data Systems's competitive position, violating regulatory requirements, damaging the company's reputation, violating contractual requirements, and posing an identity theft risk.
CONFIDENTIAL	Definition	Confidential information is highly valuable, sensitive business information and the level of protection is dictated internally by Cycom Data Systems.
	Potential Impact of Loss	**SIGNIFICANT DAMAGE** would occur if Confidential information were to become available to unauthorized parties either internal or external to Cycom Data Systems. Impact could include negatively affecting Cycom Data Systems's competitive position, damaging the company's reputation, violating contractual requirements, and exposing geographic location of individuals.
INTERNAL USE	Definition	Internal Use information is information originating within or owned by Cycom Data Systems, or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company's business interests.
	Potential Impact of Loss	**MODERATE DAMAGE** would occur if Internal Use information were to become available to unauthorized parties either internal or external to Cycom Data Systems. Impact could include damaging the company's reputation and violating contractual requirements.
PUBLIC	Definition	Public information is information that has been approved for release to the general public and is freely shareable both internally and externally.
	Potential Impact of Loss	**NO DAMAGE** would occur if Public information were to become available to parties either internal or external to Cycom Data Systems. Impact would not be damaging or a risk to business operations.

HANDLING CONTROLS PER DATA CLASSIFICATION

Handling Controls	Restricted	Confidential	Internal Use	Public
Non-Disclosure Agreement (NDA)	NDA is required prior to access by non-Cycom Data Systems employees.	- NDA is recommended prior to access by non-Cycom Data Systems employees.	- No NDA requirements	- No NDA requirements
Internal Network Transmission (wired & wireless)	- Encryption is required - Instant Messaging is prohibited - FTP is prohibited	- Encryption is recommended - Instant Messaging is prohibited - FTP is prohibited	- No special requirements	- No special requirements
External Network Transmission (wired & wireless)	- Encryption is required - Instant Messaging is prohibited - FTP is prohibited - Remote access should be used only when necessary and only with VPN and two-factor authorization when possible	- Encryption is required - Instant Messaging is prohibited - FTP is prohibited	- Encryption is recommended - Instant Messaging is prohibited - FTP is prohibited	- No special requirements
Data at Rest (file servers, databases, archives, etc.)	- Encryption is required - Logical access controls are required to limit unauthorized use - Physical access restricted to specific individuals	- Encryption is recommended - Logical access controls are required to limit unauthorized use - Physical access restricted to specific groups	- Encryption is recommended - Logical access controls are required to limit unauthorized use - Physical access restricted to specific groups	- Logical access controls are required to limit unauthorized use - Physical access restricted to specific groups
Mobile Devices (iPhone, iPad, USB Drive, etc.)	- Encryption is required - Remote wipe must be enabled, if possible	- Encryption is required - Remote wipe must be enabled, if possible	- Encryption is recommended - Remote wipe should be enabled, if possible	- No special requirements
Email (with and without attachments)	- Encryption is required - Do not forward	- Encryption is recommended - Do not forward	- Encryption is recommended - Do not forward	- No special requirements

Physical Mail	- Mark "Open by Addressee Only" - Use "Certified Mail" and sealed, tamper- resistant envelopes for external mailings	- Mark "Open by Addressee Only" - Use "Certified Mail" and sealed, tamper- resistant envelopes for external mailings	- Mail with company interoffice mail - US Mail or other public delivery systems	- No special requirements

Data Deletion Policy

SOC 2 Criteria: CC6.5

Keywords: Data Retention, Grace Period

Purpose

This policy outlines the requirements and controls/procedures Cycom Data Systems has implemented to manage the deletion of customer data.

Policy

For Customers

Customer data is retained for as long as the account is in active status. Data enters an “expired” state when the account is voluntarily closed. Expired account data will be retained for 90 days. After this period, the account and related data will be removed. Customers that wish to voluntarily close their account should download their data manually or via the API prior to closing their account.

If a customer account is involuntarily suspended, then there is a 60 day grace period during which the account will be inaccessible but can be reopened if the customer meets their payment obligations and resolves any terms of service violations.

If a customer wishes to manually backup their data in a suspended account, then they must ensure that their account is brought back to good standing so that the user interface will be available for their use. After 60 days, the suspended account will be closed and the data will enter the “expired” state. It will be permanently removed 90 days thereafter (except when required by law to retain).

Data Protection Policy

SOC 2 Criteria: CC6.1, CC6.7

Keywords: Data encryption at rest, Data encryption in transit, Data separation, Cloud monitoring

---

Background

Cycom Data Systems takes the confidentiality and integrity of its customer data very seriously and strives to assure data is protected from unauthorized access and is available when needed.

Purpose

This policy outlines many of the procedures and technical controls in support of data protection.

Scope

Production systems that create, receive, store, or transmit Cycom Data Systems customer data (hereafter "Production Systems") must follow the requirements and guidelines described in this policy.

Policy

Cycom Data Systems policy requires that:

- Data must be handled and protected according to its classification requirements and following approved encryption standards, if applicable.
- Whenever possible, store data of the same classification in a given data repository and avoid mixing sensitive and non-sensitive data in the same repository. Security controls, including authentication, authorization, data encryption, and auditing, should be applied according to the highest classification of data in a given repository.
- Employees shall not have direct administrative access to production data during normal business operations. Exceptions include emergency operations such as forensic analysis and manual disaster recovery.
- All Production Systems must disable services that are not required to achieve the business purpose or function of the system.
- All access to Production Systems must be logged.
- All Production Systems must have security monitoring enabled, including activity and file integrity monitoring, vulnerability scanning, and/or malware detection, as applicable.

Data Protection Implementation and Processes

Customer Data Protection

Cycom Data Systems hosts on Microsoft Azure in the US-Central region by default. Data is replicated across multiple regions for redundancy and disaster recovery.

All Cycom Data Systems employees adhere to the following processes to reduce the risk of compromising Production Data:

1. Implement and/or review controls designed to protect Production Data from improper alteration or destruction.
2. Ensure that confidential data is stored in a manner that supports user access logs and automated monitoring for potential security incidents.
3. Ensure Cycom Data Systems Customer Production Data is segmented and only accessible to Customer authorized to access data.
4. All Production Data at rest is stored on encrypted volumes using encryption keys managed by Cycom Data Systems.
5. Volume encryption keys and machines that generate volume encryption keys are protected from unauthorized access. Volume encryption key material is protected with access controls such that the key material is only accessible by privileged accounts.

Access

Cycom Data Systems employee access to production is guarded by an approval process and by default is disabled. When access is approved, temporary access is granted that allows access to production. Production access is reviewed by the security team on a case by case basis.

Separation

Customer data is logically separated at the database/datastore level using a unique identifier for the customer. The separation is enforced at the API layer where the client must authenticate with a chosen account and then the customer unique identifier is included in the access token and

used by the API to restrict access to data to the account. All database/datastore queries then include the account identifier.

Monitoring

Cycom Data Systems uses Azure Monitor to monitor the entire cloud service operation. If a system failure and alarm is triggered, key personnel are notified by text, chat, and/or email message in order to take appropriate corrective action.

Cycom Data Systems uses a security agent to monitor production systems. The agents monitor system activities, generate alerts on suspicious activities and report on vulnerability findings to a centralized management console.

Protecting Data At Rest

Encryption of Data at Rest

All databases, data stores, and file systems are encrypted according to Cycom Data Systems's Encryption Policy.

Protecting Data In Transit

All external data transmission is encrypted end-to-end using encryption keys managed by Cycom Data Systems. This includes, but is not limited to, cloud infrastructure and third party vendors and applications.

Encryption of Data in Transit

All internet and intranet connections are encrypted and authenticated using a strong protocol, a strong key exchange, and a strong cipher.

Data protection via end-user messaging channels

Restricted and sensitive data is not allowed to be sent over electronic end-user messaging channels such as email or chat, unless end-to-end encryption is enabled.

Disaster Recovery Plan

SOC 2 Criteria: CC5.3, CC7.5

Keywords: Tabletop testing, Disaster Recovery Simulation

Purpose

This policy establishes procedures to recover Cycom Data Systems following a disruption resulting from a disaster. This Disaster Recovery Policy is maintained by the Cycom Data Systems Security Officer and Privacy Officer.

Background

The following objectives have been established for this plan:

1. Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
    1. **Notification/Activation phase** to detect and assess damage and to activate the plan.
    2. **Recovery phase** to restore temporary operations and recover damage done to the original system.
    3. **Reconstitution phase** to restore system processing capabilities to normal operations.
2. Identify the activities, resources, and procedures needed to carry out Cycom Data Systems processing requirements during prolonged interruptions to normal operations.
3. Identify and define the impact of interruptions to Cycom Data Systems systems.
4. Assign responsibilities to designated personnel and provide guidance for recovering Cycom Data Systems systems during prolonged periods of interruption to normal operations.
5. Ensure coordination with other Cycom Data Systems staff who will participate in the Disaster Recovery Planning strategies.
6. Ensure coordination with external points of contact and vendors who will participate in the Disaster Recovery Planning strategies.

Policy

Examples of the types of disasters that would initiate this plan are natural disaster, political disturbances, human-made disaster, external human threats, internal malicious activities.

Cycom Data Systems defines two categories of systems from a disaster recovery perspective:

1. **Critical Systems**.

These systems host application servers and database servers or are required for functioning of systems that host application servers and database servers. These systems, if unavailable, affect the integrity of data and must be restored, or have a process begun to restore them, immediately upon becoming unavailable.

1. **Non-critical Systems**.

These are all systems not considered critical by the definition above. These systems, while they may affect the performance and overall security of critical systems, do not prevent Critical systems from functioning and being accessed appropriately. These systems are restored at a lower priority than critical systems.

Threat and Risk Assessment and Management

There are many potential disruptive threats which can occur at any time and affect the normal business process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency situation has been examined. The focus here is on the level of business disruption which could arise from each type of disaster.

The Cycom Data Systems IT Risk Assessment documents a full detailed assessment of threats.

Testing and Maintenance

The Security Officer shall establish criteria for validation/testing of a Disaster Recovery Plan, an annual test schedule, and ensure implementation of the test. This process will also serve as training for personnel involved in the plan's execution. At a minimum, the Disaster Recovery Plan shall be tested annually. The types of validation/testing exercises include tabletop and technical testing.

Tabletop Testing

The primary objective of the tabletop test is to ensure designated personnel are knowledgeable and capable of performing the notification/activation requirements and procedures as outlined in the Disaster Recovery Plan, in a timely manner. The exercises include, but are not limited to:

- Testing to validate the ability to respond to a crisis in a coordinated, timely, and effective manner, by simulating the occurrence of a specific crisis.

Technical Testing

The primary objective of the technical test is to ensure the communication processes and data storage and recovery processes can function at an alternate site to perform the functions and capabilities of the system within the designated requirements. Technical testing shall include, but is not limited to:

- Process from backup system at the alternate site
- Restore system using backups
- Switch compute and storage resources to alternate processing site.

Disaster Recovery Procedures

Notification and Activation Phase

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to Cycom Data Systems. Based on the assessment of the Event, sometimes according to the Cycom Data Systems Incident Response Policy, the Disaster Recovery Plan may be activated by the Security Officer and/or CTO.

The notification sequence is listed below:

- The first responder is to notify the CTO. All known information must be relayed to the CTO.
- The CTO is to contact the rest of the team and inform them of the event. The CTO is to begin assessment procedures.
- The CTO is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the CTO is to follow the steps below.

Damage Assessment Procedures:

- The CTO is to logically assess damage, gain insight into whether the infrastructure is salvageable, and begin to formulate a plan for recovery.

Alternate Assessment Procedures:

- Upon notification, the CTO is to follow the procedures for damage assessment with combined DevOps and Web Services Teams.
- The Cycom Data Systems Disaster Recovery Plan is to be activated if one or more of the following criteria are met:
  - Cycom Data Systems systems will be unavailable for more than 48 hours.
  - Hosting facility is damaged and will be unavailable for more than 24 hours.
  - Other criteria, as appropriate and as defined by Cycom Data Systems.
- If the plan is to be activated, the CTO is to notify and inform team members of the details of the event and if relocation is required.
- Upon notification from the CTO, group leaders and managers are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.
- The CTO is to notify the hosting facility partners that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the alternate site.
- The CTO is to notify remaining personnel and executive leadership on the general status of the incident.
- Notification can be delivered via message, email, or phone.

Recovery Phase

This section provides procedures for recovering the application at an alternate site, whereas other efforts are directed to repair damage to the original system and capabilities.

The following procedures are for recovering the Cycom Data Systems infrastructure at the alternate site. Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

Recovery Goal: The goal is to rebuild Cycom Data Systems infrastructure to a production state.

The tasks outlined below are not sequential and some can be run in parallel.

1. Contact Partners and Customers affected.
2. Assess damage to the environment.
3. Begin replication of new environment using automated and tested scripts. At this point it is determined whether to recover in Rackspace, AWS, GCP, Heroku, Azure, or another cloud environment.
4. Test new environment using pre-written tests.
5. Test logging, security, and alerting functionality.
6. Assure systems are appropriately patched and up to date.
7. Deploy environment to production.
8. Update DNS to new environment.

Reconstitution Phase

This section discusses activities necessary for restoring Cycom Data Systems operations at the original or new site. The goal is to restore full operations within 24 hours of a disaster or outage. When the hosted data center at the original or new site has been restored, Cycom Data Systems operations at the alternate site may be transitioned back. The goal is to provide a seamless transition of operations from the alternate site to the computer center.

Original or New Site Restoration

- Begin replication of new environment using automated and tested scripts - DevOps
- Test new environment using pre-written tests. - Web Services
- Test logging, security, and alerting functionality. - Dev Ops
- Deploy environment to production - Web Services
- Assure systems are appropriately patched and up to date. - Dev Ops
- Update DNS to new environment. - Dev Ops

Plan Deactivation

If the Cycom Data Systems environment is moved back to the original site from the alternative site, all hardware used at the alternate site should be handled and disposed of according to Cycom Data Systems policy.

Encryption Policy

Keywords: Encryption key management

Purpose

This policy defines organizational requirements for the use of cryptographic controls, as well as the requirements for cryptographic keys, in order to protect the confidentiality, integrity, authenticity, and nonrepudiation of information.

Scope

This policy applies to all systems, equipment, facilities and information within the scope of Cycom Data Systems's information security program. All employees, contractors, part-time, and temporary workers, service providers, and those employed by others to perform work on behalf of the organization having to do with cryptographic systems, algorithms, or keying material are subject to this policy and must comply with it.

Background

This policy defines the high level objectives and implementation instructions for Cycom Data Systems's use of cryptographic algorithms and keys. It is vital that the organization adopt a standard approach to cryptographic controls across all work centers in order to ensure end-to-end security, while also promoting interoperability. This document defines the specific algorithms approved for use, requirements for key management and protection, and requirements for using cryptography in cloud environments.

Policy

Cryptography Controls

Cycom Data Systems must protect individual systems or information by means of cryptographic controls as defined in Table 3:

Table 3: Cryptographic Controls

Name of System/Type of Information	Cryptographic Tool	Encryption Algorithm	Key Size
Public Key Infrastructure for Authentication	OpenSSL	AES-256	256-bit key
Data Encryption Keys	OpenSSL	AES-256	256-bit key
Virtual Private Network (VPN) keys	OpenSSL and OpenVPN	AES-256	256-bit key
Website SSL Certificate	OpenSSL, CERT	AES-256	256-bit key

Keys

Except where otherwise stated, keys must be managed by their owners. Cryptographic keys must be protected against loss, change or destruction by applying appropriate access control mechanisms to prevent unauthorized use and backing up keys on a regular basis.

Obtaining Information

When required, customers of Cycom Data Systems's cloud-based software platform offering must be able to obtain information regarding:

- The cryptographic tools used to protect their information.
- Any capabilities that are available to allow cloud service customers to apply their own cryptographic solutions.
- The identity of the countries where the cryptographic tools are used to store or transfer cloud service customers' data.

Governing Law

The use of organizationally-approved encryption must be governed in accordance with the laws of the country, region, or other regulating entity in which users perform their work. Encryption must not be used to violate any laws or regulations including import/export restrictions. The encryption used by Cycom Data Systems conforms to international standards and U.S. import/export requirements, and thus can be used across international boundaries for business purposes.

Key Management Service

All key management must be performed using software that automatically manages key generation, access control, secure storage, backup and rotation of keys. Specifically:

- The key management service must provide key access to specifically-designated users, with the ability to encrypt/decrypt information and generate data encryption keys.
- The key management service must provide key administration access to specifically-designated users, with the ability to create, schedule delete, enable/disable rotation, and set usage policies for keys.
- The key management service must store and backup keys for the entirety of their operational lifetime.
- The key management service must rotate keys at least once every 12 months.

Incident Response Plan

SOC 2 Criteria: CC2.2, CC2.3, CC4.2, CC5.1, CC7.3, CC7.5, CC9.1

Keywords: Impact, Security impact level, Report template, Incident

---

Purpose

This security incident response policy is intended to establish controls to ensure detection of security vulnerabilities and incidents, as well as quick reaction and response to security breaches.

This document also provides implementing instructions for security incident response, to include definitions, procedures, responsibilities, and performance measures (metrics and reporting mechanisms).

Scope

This policy applies to all users of information systems within Cycom Data Systems. This typically includes employees and contractors, as well as any external parties that come into contact with systems and information controlled by Cycom Data Systems (hereinafter referred to as “users”). This policy must be made readily available to all users.

Background

A key objective of Cycom Data Systems’s Information Security Program is to focus on detecting information security weaknesses and vulnerabilities so that incidents and breaches can be prevented wherever possible. Cycom Data Systems is committed to protecting its employees, customers, and partners from illegal or damaging actions taken by others, either knowingly or unknowingly. Despite this, incidents and data breaches are likely to happen; when they do, Cycom Data Systems is committed to rapidly responding to them, which may include identifying, containing, investigating, resolving , and communicating information related to the breach.

This policy requires that all users report any perceived or actual information security vulnerability or incident as soon as possible using the contact mechanisms prescribed in this document. In addition, Cycom Data Systems must employ automated scanning and reporting mechanisms that can be used to identify possible information security vulnerabilities and incidents. If a vulnerability is identified, it must be resolved within a set period of time based on its severity. If an incident is identified, it must be investigated within a set period of time based on its severity. If an incident is confirmed as a breach, a set procedure must be followed to contain, investigate, resolve, and communicate information to employees, customers, partners and other stakeholders.

Within this document, the following definitions apply:

- **Information Security Vulnerability:**

A vulnerability in an information system, information system security procedures, or administrative controls that could be exploited to gain unauthorized access to information or to disrupt critical processing.

- **Information Security Incident:**

A suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of information security policy.

Policy

- All users must report any system vulnerability, incident, or event pointing to a possible incident to the Security Officer as quickly as possible but no later than 24 hours.
- Incidents must be reported by sending an email message with details of the incident.
- Users must be trained on the procedures for reporting information security incidents or discovered vulnerabilities, and their responsibilities to report such incidents. Failure to report information security incidents shall be considered to be a security violation and will be reported to the Human Resources (HR) Manager for disciplinary action.
- Information and artifacts associated with security incidents (including but not limited to files, logs, and screen captures) must be preserved in the event that they need to be used as evidence of a crime.
- All information security incidents must be responded to through the incident management procedures defined below.

Periodic Evaluation

It is important to note that the processes surrounding security incident response should be periodically reviewed and evaluated for effectiveness. This also involves appropriate training of resources expected to respond to security incidents, as well as the training of the general population regarding Cycom Data Systems's expectation for them, relative to security responsibilities. The incident response plan is tested annually.

Procedure For Establishing Incident Response System:

1. Define on-call schedule and assign an Information Security Manager (ISM) responsible for managing incident response procedure during each availability window.
2. Define notification channel to alert the on-call ISM of a potential security incident. Establish a company resource that includes up to date contact information for on-call ISM.
3. Assign management sponsors from the Engineering, Legal, HR, Marketing, and C-Suite teams.
4. Distribute Procedure For Executing Incident Response to all staff and ensure up-to-date versions are accessible in a dedicated company resource.
5. Require all staff to complete training for Procedure For Executing Incident Response at least once per year.

Procedure For Executing Incident Response:

1. When an information security incident is identified or detected, users must notify their immediate manager within 24 hours. The manager must immediately notify the ISM on call for proper response. The following information must be included as part of the notification:
    1. Description of the incident
    2. Date, time, and location of the incident
    3. Person who discovered the incident
    4. How the incident was discovered
    5. Known evidence of the incident
    6. Affected system(s)
2. Within 48 hours of the incident being reported, the ISM shall conduct a preliminary investigation and risk assessment to review and confirm the details of the incident. If the incident is confirmed, the ISM must assess the impact to Cycom Data Systems and assign a severity level, which will determine the level of remediation effort required:
    1. **High**: the incident is potentially catastrophic to Cycom Data Systems and/or disrupts Cycom Data Systems's day-to-day operations; a violation of legal, regulatory or contractual requirements is likely.
    2. **Medium**: the incident will cause harm to one or more business units within Cycom Data Systems and/or will cause delays to a business unit's activities.
    3. **Low**: the incident is a clear violation of organizational security policy, but will not substantively impact the business.
3. The ISM, in consultation with management sponsors, shall determine appropriate incident response activities in order to contain and resolve incidents.
4. The ISM must take all necessary steps to preserve forensic evidence (e.g. log information, files, images) for further investigation to determine if any malicious activity has taken place. All such information must be preserved and provided to law enforcement if the incident is determined to be malicious.
5. If the incident is deemed as High or Medium, the ISM must work with the VP Brand/Creative, General Counsel, and HR Manager to create and execute a communications plan that communicates the incident to users, the public, and others affected.
6. The ISM must take all necessary steps to resolve the incident and recover information systems, data, and connectivity. All technical steps taken during an incident must be documented in Cycom Data Systems's incident log, and must contain the following:
    1. Description of the incident
    2. Incident severity level
    3. Root cause (e.g. source address, website malware, vulnerability)
    4. Evidence
    5. Mitigations applied (e.g. patch, re-image)
    6. Status (open, closed, archived)
    7. Disclosures (parties to which the details of this incident were disclosed to, such as customers, vendors, law enforcement, etc.)
7. After an incident has been resolved, the ISM must conduct a post-mortem that includes root cause analysis and documentation of any lessons learned.
8. Depending on the severity of the incident, the Chief Executive Officer (CEO) may elect to contact external authorities, including but not limited to law enforcement, private investigation firms, and government organizations as part of the response to the incident.
9. The ISM must notify all users of the incident, conduct additional training if necessary, and present any lessons learned to prevent future occurrences. Where necessary, the HR Manager must take disciplinary action if a user's activity is deemed as malicious.

Appendix A: Security Incident Report Template

1.0 Reported By

1.1 Last Name:
1.2 First Name:
1.3 Position:
1.4 Company/Org Name:
1.5 Telephone No:
1.6 E-mail:

2.0 Organization Details

3.0 Incident Details including Injury and Impact Level

4.0 Status of Mitigation Actions

5.0 Computer Network Defense Incident Type (if applicable)

2.1 Name of organization:	
2.2 Type of organization:	

2.3 Street Address:	
2.4 At this time, is it known that other organizations are affected by this incident? (If so, list names, addresses, telephone number, email addresses and contact persons):	

3.1 Date:	3.2 Time:	
3.3 Location of affected site:		
3.4 Brief summary of the incident (what has happened, where did it happen, when did it happen):		
3.5 Description of the project/program and information involved, and, if applicable, the name of the specific program:		
3.6 Classification level of the information involved		
3.7 System compromise (detail):		
3.8 Data compromise (detail):		
3.9 Originator and /or Official Classification Authority of the information involved? (List name, address, telephone no., email and contact person).		
3.10 Is Foreign Government Information involved? Originating country or International organization?		
3.11 Did the incident occur on an accredited system authorized to process and store the information in question?		
3.12 Estimated injury level/sector:		
3.13 Estimated impact level: (any compromise or disruption to service?)		
3.14 Incident duration:		
3.15 Estimated number of systems affected:		
3.16 Percentage of organization systems affected:		
3.17 Action taken:		
3.18 Supporting documents attached (describe if any)		
3.19 Multiple occurrence or first time this type of incident occurs within this location?		
3.20 Incident Status (resolved or unresolved)		
3.21 Has the matter been reported to other authorities? If so, list names, addresses, telephone no., email and contact person.		

4.1 Mitigation details to date: (List any actions that have been taken to mitigate incident and by whom)	
4.2 Results of mitigation:	
4.3 Additional assistance required?	

5.1 Malicious code: (Worm, virus, trojan, backdoor, rootkit, etc.)				
5.2 Known vulnerability exploit: (List the Common Vulnerabilities and Exposures (CVE) number for known vulnerability)				
5.3 Disruption of service:				
5.4 Access violation: (Unauthorized access attempt, successful unauthorized access, password cracking, Etc.)				
5.5 Accident or error: (Equipment failure, operator error, user error, natural or accidental causes)				
5.6 If the incident resulted from user error or malfeasance, identify reasons (training, disregard for policy, other) and responsible parties				
5.7 Additional details:				
5.8. Apparent Origin of Incident or Attack	Source IP and port:		Protocol:	

	URL:		Malware:	
	Additional details:			

6.0 Systems Affected

6.1 Network zone affected: (Internet, administration, internal, etc.)	
6.2 Type of system affected: (File server, Web server, mail server, database, workstation (mobile or desktop), etc.)	
6.3 Operating system (specify version):	
6.4 Protocols or services:	
6.5 Application (specify version):	

7.0 Post Incident Activities

7.1 Has information contained in this report been provided to the authorities? When?	
7.2 Complete a root cause analysis to determine the reason for the incident and steps to prevent re-occurrence.	

Information Security Policy

SOC 2 Criteria: CC1.2, CC1.3, CC2.1, CC5.1, CC5.2, CC5.3,

Keywords: Corrective action, Security training, Clean desk

Background

It is the policy of Cycom Data Systems that information, as defined hereinafter, in all its forms--written, spoken, recorded electronically or printed--will be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life-cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information.

The Security Officer is responsible for the design, development, maintenance, dissemination, and enforcement of the items contained in this policy. At minimum on an annual basis, a security and/ or compliance committee composed of senior management and key personnel must discuss, evaluate and document the company's security program, ensuring strategic goals and objectives are continually being developed. At a minimum on an annual basis, all policies must be reviewed, modified and/ or edited to meet necessary security standards. All policies must be signed and approved by authorized personnel.

Policies and/or procedures must be accessible to employees for review at all times via the compliance automation SaaS, Drata. Policies pertaining to positions must be reviewed and signed upon hire and on an annual basis by all employees.

Requests for any exceptions to any policies included within the security program must be approved by Executive Management. Any approved exceptions will be reviewed annually.

Purpose

This Policy has been developed to meet the company's regulatory, legal, contractual, and other obligations; to ensure that the appropriate company image is presented, and to control business risks.

Scope

This Policy applies to:

- Information in any form, regardless of the media on which it is stored, as well as, any facility, system, or network used to store, process, and/or transfer information.
- All Cycom Data Systems employees, temporary staff, partners, contractors, vendors, suppliers, and any other person (collectively also referred to as "Staff" or "Personnel") or entity that accesses the company's networks or any other public or private network through company's networks or systems.
- All activity while using or accessing the company's information or information processing, storage, or transmission equipment, while on the company premises (owned, rented, leased, or borrowed) or remotely.
- Information resources that have been entrusted to the company by any entity external to the company (i.e. Customers, Staff, and others).
- **Documents, messages, and other communications created on or communicated via the company systems are considered the company's business records and, as such, are subject to review by third parties in relation to audits, litigation, process improvement, and compliance.**

Training

Management shall ensure that employees, contractors and third party users:

- Are properly briefed on their information security roles and responsibilities prior to being granted access to covered information or information systems;
- Are provided with guidelines which state security expectations of their role within the organization;
- Are motivated and comply with the security policies of the organization;
- Achieve a level of awareness on security relevant to their roles and responsibilities within the organization;
- Conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate methods of working.

All new hires are required to complete information security awareness training as part of their new employee onboarding process and annually thereafter. New hire onboarding will be completed within **30 days** after the date the employee or contractor is hired. Ongoing training will include security and privacy requirements as well as training in the correct use of information assets and facilities.

Additional specialized training will be required for individuals responsible for maintaining system security. Specialized topics would include spam, phishing, OWASP Top Ten list, and SANS Top 25 list. In addition, consistent with assigned roles and responsibilities, incident response and contingency training to personnel will be done:

I. within 90 days of assuming an incident response role or responsibility;

II. as required by information system or policy changes; and

III. once a year thereafter.

The organization will document that the training has been provided to all employees.

All employees are required to acknowledge in writing their understanding of the Information Security Program which includes a Code of Conduct upon hire and annually thereafter.

Clean Desk/Work Area Policy

- Authorized users will ensure that all sensitive/confidential materials are removed from their workspace and locked away when the items are not in use or an employee leaves his/her workstation.
- Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
- Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
- Whiteboards containing Restricted and/or Sensitive information should be erased.
- Treat mass storage devices such as external hard drives or USB drives as sensitive and always secure and encrypt them.
- All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

Internet/Intranet Access and Use

Use of Cycom Data Systems computers, networks, and Internet access is a privilege granted by management and may be revoked at any time for inappropriate conduct carried out on such systems, including, but not limited to:

- Sending chain letters or participating in any way in the creation or transmission of unsolicited "spam" that is unrelated to legitimate Company purposes;
- Engaging in private or personal business activities, including excessive use of instant messaging and chat rooms;
- Accessing networks, servers, drives, folders, or files to which the employee has not been granted access or authorization from someone with the right to make such a grant;
- Making unauthorized copies of Company files or other Company data;
- Destroying, deleting, erasing, or concealing Company files or other Company data, or otherwise making such files or data unavailable or inaccessible to the Company or to other authorized users of Company systems;
- Misrepresenting oneself or the Company;
- Violating the laws and regulations of federal, state, city, province, or local jurisdictions in any way;
- Engaging in unlawful or malicious activities;
- Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the Company's networks or systems or those of any other individual or entity;
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;
- Sending, receiving, or accessing pornographic materials;
- Causing congestion, disruption, disablement, alteration, or impairment of Company networks or systems;
- Using recreational games; and/or
- Defeating or attempting to defeat security restrictions on company systems and applications.

Enforcement

Cycom Data Systems Management, under the explicit authority granted by the company CEO, retains the authority and responsibility to monitor and enforce compliance with this Policy and other policies, standards, procedures, and guidelines. Monitoring activities may be conducted on an on-going basis or on a random basis whenever deemed necessary by Management and may require investigating the use of the Company’s information resources. The company reserves the right to review any and all communications and activities without notice.

Cycom Data Systems will take appropriate precautions to ensure that monitoring activities are limited to the extent necessary to determine whether the communications or activities are in violation of Company policies, standards, procedures, and guidelines or in accordance with normal business processing performance or quality activities.

Violation of the controls established in this Policy is prohibited and will be appropriately addressed. Disciplinary actions for violations may include verbal and/or written warnings, suspension, termination, and/or other legal remedies and will be consistent with our published HR standards and practices.

Employee Sanctions

Cycom Data Systems’s discipline policy and procedures are designed to provide a structured corrective action process to improve and prevent a recurrence of undesirable employee behavior and performance issues. It has been designed to be consistent with Cycom Data Systems cultural values, Human Resources (HR) best practices, and employment laws.

Cycom Data Systems reserves the right to combine or skip steps depending on the facts of each situation and the nature of the offense. The level of disciplinary intervention may also vary. Some of the factors that will be considered are whether the offense is repeated despite coaching, counseling, or training, the employee’s work record, and the impact the conduct and performance issues have on the organization.

Corrective Action Procedure

Step 1: Verbal Warning and Counseling

This initial step creates an opportunity for the immediate supervisor to schedule a meeting with an employee to bring attention to an existing performance, conduct or attendance issue. The supervisor should discuss with the employee the nature of the problem or the violation of company policies and procedures. The supervisor is expected to clearly describe expectations and the steps the employee must take to improve performance or resolve the problem.

Step 2: Formal Written Warning

If the employee does not promptly correct any performance, conduct or attendance issues that were identified in Step 1, a written warning will become formal documentation of the performance, conduct, or attendance issues and consequences. The employee will sign a copy of the document to acknowledge receipt and understanding of the formal warning. During Step 2, the immediate supervisor and HR representative will meet with the employee to review any additional incidents or information about the performance, conduct or attendance issues as well as any prior relevant corrective action plans. Management will outline the consequences for the employee of his or her continued failure to meet performance or conduct expectations.

A formal performance improvement plan (PIP) requiring the employee's immediate and sustained corrective action will be issued after a Step 2 meeting. A warning outlining that the employee may be subject to additional discipline up to and including termination if immediate and sustained corrective action is not taken may also be included in the written warning.

Step 3: Suspension and Final Written Warning

There may be performance, conduct, or safety incidents so problematic and harmful that the most effective action may be the temporary removal of the employee from the workplace. When immediate action is necessary to ensure the safety of the employee or others, the immediate supervisor may suspend the employee pending the results of an investigation. Suspensions that are recommended as part of the normal progression of this progressive discipline policy and procedure are subject to approval from a next-level manager and HR.

Step 4: Recommendation for Termination of Employment

The last step in the progressive discipline procedure is a recommendation to terminate employment. Generally, Cycom Data Systems will try to exercise the progressive nature of this policy by first providing warnings, a final written warning or suspension from the workplace before proceeding to a recommendation to terminate employment. However, Cycom Data Systems reserves the right to combine and skip steps depending on the circumstances of each situation and the nature of the offense. Furthermore, employees may be terminated without prior notice or disciplinary action.

Management's recommendation to terminate employment must be approved by HR and the supervisor's immediate manager. Final approval may be required from the CEO.

Performance and Conduct Issues Not Subject to Progressive Discipline

Behavior that is illegal is not subject to progressive discipline, and such behavior may be reported to local law enforcement authorities. Theft, substance abuse, intoxication, fighting and other acts of violence at work are grounds for immediate termination.

Password Policy

SOC 2 Criteria: CC6.1

Keywords: Password requirements, Password Manager, Complex passwords, 2FA, MFA

Purpose

This policy describes the procedure to select and securely manage passwords at Cycom Data Systems.

Scope

This policy applies to all Cycom Data Systems employees, contractors, and any other personnel who have an account on any system that resides at any company facility or has access to the company network.

Policy

If a password is suspected of being compromised, the password in question should be rotated and the Security Officer should be notified immediately.

Password Requirements

- Complex passwords are required where possible. Complex passwords have at least 10 characters, 1+ uppercase letter(s), 1+ lowercase letter(s), 1+ non-alphanumeric character(s)
- Passwords must have at least 8 characters
- Do not reuse previously used passwords or their variants
- Do not use commonly used passwords

MFA Requirements

- MFA must be enabled for any and all systems that provide the option for Multi-Factor Authentication (MFA)

Password Protection

- All passwords are treated as confidential information and should not be shared with anyone. If you receive a request to share a password, deny the request and contact the system owner for assistance in provisioning an individual user account.
- Do not write down passwords, store them in emails, electronic notes, or mobile devices, or share them over the phone. If you must store passwords electronically, do so with a password manager that has been approved by Cycom Data Systems:
- Cycom Data Systems's approved Password Manager: LastPass or Norton Password Manager
- If you absolutely must share a password, do so through the approved password manager or grant access to an application through a single-sign-on (SSO) provider.
- If you suspect a password has been compromised, rotate the password immediately and notify the Company's Security Officer.
- Passwords stored in systems must be stored with a unique salt and as a one-way hash using an approved password hashing algorithm (pbkdf2, bcrypt, scrypt) and an HMAC-SHA256

Enforcement

- An employee or contractor found to have violated this policy may be subject to disciplinary action.

Physical Security Policy

SOC 2 Criteria: CC6.4

Keywords: Facilities, Office visitors

Background

It is the goal of Cycom Data Systems to provide a safe and secure environment for all employees. Access to the Cycom Data Systems facilities is limited to authorized individuals only. All workforce members are responsible for reporting an incident of unauthorized visitor and/or unauthorized access to Cycom Data Systems's facility.

Purpose and Scope

Cycom Data Systems policy requires that:

- Physical access to Cycom Data Systems facilities is restricted.
- All employees are required to wear employee badges at secure facilities if and when applicable (such as server rooms, data centers, labs).
- All employees must follow physical security requirements and procedures documented by facility management.
- On-site visitors and vendors must be escorted by a Cycom Data Systems employee at all times while on premise.
- All workforce members are responsible for reporting an incident of unauthorized visitor and/or unauthorized access to Cycom Data Systems's facility.
- A record is retained for each physical access, including visits, maintenance and repairs to Cycom Data Systems production environments and secure facilities.
    - Details must be captured for all maintenance and repairs performed to physical security equipment such as locks, walls, doors, surveillance cameras; and
    - All records must be retained for a minimum of seven years.
- Building security, such as fire extinguishers and detectors, escape routes, floor warden responsibilities, shall be maintained according to applicable laws and regulations.

Policy

Physical Security

Access Requirements Overview

- Physical access is restricted using badge readers and/or smart locks that track all access.
    - Restricted areas and facilities are locked when unattended (where feasible).
    - Only authorized workforce members receive access to restricted areas (as determined by the Security Officer).
    - Access and keys are revoked upon termination of workforce members.
    - Workforce members must report a lost and/or stolen key(s) or badge(s) to his/her manager, local Site Lead, or the Facility Manager.
    - The Facility Manager or designee is responsible to revoke access to the lost/stolen badge(s) or access key(s), and re-provision access as needed.
    - The Facility Manager or designee facilitates the changing of the lock(s) within 7 days of a physical key being reported lost/stolen.
- Enforcement of Facility Access Policies
    - Report violations of this policy to the restricted area's department team leader, supervisor, manager, or director, or the Privacy Officer.
    - Workforce members in violation of this policy are subject to disciplinary action, up to and including termination.
    - Visitors in violation of this policy are subject to loss of vendor privileges and/or termination of services from Cycom Data Systems.
- Workstation Security
    - Workstations may only be accessed and utilized by authorized workforce members to complete assigned job/contract responsibilities.
    - All workforce members are required to monitor workstations and report unauthorized users and/or unauthorized attempts to access systems/applications as per the System Access Control Policy.
    - All workstations purchased by Cycom Data Systems are the property of Cycom Data Systems and are distributed to personnel by the company.
- Home Office Security
    - Friends and family are not permitted to use work devices.
    - Work devices are not to be left in an unsecure location. Follow the same physical security habits that you would in a work setting: lock your screen when away from your computer, lock your doors, and do not leave your devices in the car.
    - Work devices are not to be left unattended and must be placed in a secure location when not in use.
    - Sensitive data must not be stored on portable drives.
    - Sensitive data must not be printed or otherwise rendered on unsecured media.
    - Immediately report lost or stolen work devices to the Security Officer.

- When traveling for an extended period of time, all work devices should be taken with you or stored in a locked and secure location.

Data Center Security

Physical security of data centers is ensured by Cycom Data Systems’s cloud infrastructure service provider.

Responsible Disclosure Policy

SOC 2 Criteria: CC2.2, CC5.3

Cycom Data Systems is committed to ensuring the safety and security of our customers. We aim to foster an open partnership with the security community, and we recognize that the work the community does is important in continuing to ensure safety and security for all of our customers. We have developed this policy to both reflect our corporate values and to uphold our legal responsibility to good-faith security researchers that are providing us with their expertise.

Scope

Cycom Data Systems' Responsible Disclosure Policy covers the following products:

- Cycom Data Systems' core platform

We intend to increase our scope as we build capacity and experience with this process. Researchers who submit a vulnerability report to us will be given full credit on our website once the submission has been accepted and validated by our product security team.

Legal Posture

Cycom Data Systems will not engage in legal action against individuals who submit vulnerability reports through our Vulnerability Reporting inbox. We openly accept reports for the currently listed Cycom Data Systems products. We agree not to pursue legal action against individuals who:

- Engage in testing of systems/research without harming Cycom Data Systems or its customers.
- Engage in vulnerability testing within the scope of our vulnerability disclosure program.
- Test on products without affecting customers, or receive permission/consent from customers before engaging in vulnerability testing against their devices/software, etc.
- Adhere to the laws of their location and the location of Cycom Data Systems. For example, violating laws that would only result in a claim by Cycom Data Systems (and not a criminal claim) may be acceptable as Cycom Data Systems is authorizing the activity (reverse engineering or circumventing protective measures) to improve its system.
- Refrain from disclosing vulnerability details to the public before a mutually agreed-upon timeframe expires.

How to Submit a Vulnerability

To submit a vulnerability report to Cycom Data Systems' Product Security Team, please utilize the following email: security@cycominc.com.

Preference, Prioritization, and Acceptance Criteria

We will use the following criteria to prioritize and triage submissions.

What we would like to see from you:

- Well-written reports in English will have a higher probability of resolution.
- Reports that include proof-of-concept code equip us to better triage.
- Reports that include only crash dumps or other automated tool output may receive lower priority.
- Reports that include products not on the initial scope list may receive lower priority.
- Please include how you found the bug, the impact, and any potential remediation.
- Please include any plans or intentions for public disclosure.

What you can expect from Cycom Data Systems:

- A timely response to your email (within 2 business days).
- After triage, we will send an expected timeline, and commit to being as transparent as possible about the remediation timeline as well as on issues or challenges that may extend it.
- An open dialog to discuss issues.
- Notification when the vulnerability analysis has completed each stage of our review.
- Credit after the vulnerability has been validated and fixed.

If we are unable to resolve communication issues or other problems, Cycom Data Systems may bring in a neutral third party to assist in determining how best to handle the vulnerability.

Risk Assessment Policy

SOC 2 Criteria: CC3.1, CC1.2, CC2.1, CC3.1, CC3.2, CC3.3, CC3.4, CC4.1, CC4.2, CC5.1, CC5.2, CC5.3

Keywords: Risk assessment, Threat impact, Threat likelihood, Risk score, Risk remediation

---

Purpose

The purpose of this policy is to define the methodology for the assessment and treatment of information security risks within Cycom Data Systems, and to define the acceptable level of risk as set by Cycom Data Systems's leadership.

Scope

Risk assessment and risk treatment are applied to the entire scope of Cycom Data Systems's information security program, and to all assets which are used within Cycom Data Systems or which could have an impact on information security within it. This policy applies to all employees of Cycom Data Systems who take part in risk assessment and risk treatment.

Background

A key element of Cycom Data Systems's information security program is a holistic and systematic approach to risk management. This policy defines the requirements and processes for Cycom Data Systems to identify information security risks. The process consists of four parts: identification of Cycom Data Systems's assets, as well as the threats and vulnerabilities that apply; assessment of the likelihood and consequence (risk) of the threats and vulnerabilities being realized, identification of treatment for each unacceptable risk, and evaluation of the residual risk after treatment.

Policy

Risk Assessment

- The risk assessment process includes the identification of threats and vulnerabilities having to do with company assets.
- The first step in the risk assessment is to identify all assets within the scope of the information security program; in other words, all assets which may affect the confidentiality, integrity, and/or availability of information in the organization. Assets may include documents in paper or electronic form, applications, databases, information technology equipment, infrastructure, and external/outsourced services and processes. For each asset, an owner must be identified.
- The next step is to identify all threats and vulnerabilities associated with each asset. Threats and vulnerabilities must be listed in a risk assessment table. Each asset may be associated with multiple threats, and each threat may be associated with multiple vulnerabilities.
- For each risk, an owner must be identified. The risk owner and the asset owner may be the same individual.
- Once risk owners are identified, they must assess:
    - Impact for each combination of threats and vulnerabilities for an individual asset if such a risk materializes.
    - Likelihood of occurrence of such a risk (i.e. the probability that a threat will exploit the vulnerability of the respective asset).
    - Criteria for determining impact and likelihood are defined in the tables below.
- The risk level is calculated by multiplying the impact score and the likelihood score.

Description of Impact Levels and Criteria:

Impact (Score)	Definition
Incidental (1.0)	• Minimal financial loss • Local media attention quickly remedied • Not reportable to regulator • Isolated staff dissatisfaction
Minor (2.0)	• Minor financial loss • Local reputational damage • Reportable incident to regulator, no follow up • General staff morale problems and increase in turnover
Moderate (3.0)	• Moderate financial loss • National short-term negative media coverage • Report of breach to regulator with immediate correction to be implemented • Widespread staff morale problems and high turnover
Major (4.0)	• Significant financial loss • National long-term negative media coverage; significant loss of market share • Report to regulator requiring major project for corrective action • Some senior managers leave, high turnover of experienced staff, not perceived as employer of choice
Extreme (5.0)	• Massive financial loss over • International long-term negative media coverage; game-changing loss of market share • Significant prosecution and fines, litigation including class actions, incarceration of leadership • Multiple senior leaders leave

Description of Likelihood Levels and Criteria:

Likelihood (Weight Factor)	Definition
Rare (1.0)	Once in 100 years or less (<10% chance of occurrence over the life of the company)
Unlikely (2.0)	Once in 50 to 100 years (10% to 35% chance of occurrence over the life of the company)
Possible (3.0)	Once in 25 to 50 years (35% to 65% chance of occurrence over the life of the company)
Likely (4.0)	Once in 2 to 25 years (65% to 90% chance of occurrence over the life of the company)
Almost Certain (5.0)	Up to once in 2 years or more (90% or greater chance of occurrence over the life of the company)

Risk Rating Criteria:

Risk Rating:
Low Risk: Less than or equal to 4.0
Medium Risk: Greater than 4.0 but less than or equal to 9.0
High Risk: Greater than 9.0 but less than or equal to 16.0
Critical Risk: Greater than 16.0

Risk Rating Matrix:

RISK SCORE MATRIX						
		Impact				
		INCIDENTAL (1.0)	**MINOR (2.0)**	**MODERATE (3.0)**	**MAJOR (4.0)**	**EXTREME (5.0)**
Likelihood	**RARE (1.0)**	**LOW** 1.0 x 1.0 = 1.0	**LOW** 1.0 x 2.0 = 2.0	**LOW** 1.0 x 3.0 = 3.0	**MEDIUM** 1.0 x 4.0 = 4.0	**MEDIUM** 1.0 x 5.0 = 5.0
	UNLIKELY (2.0)	**LOW** 2.0 x 1.0 = 2.0	**MEDIUM** 2.0 x 2.0 = 4.0	**MEDIUM** 2.0 x 3.0 = 6.0	**MEDIUM** 2.0 x 4.0 = 8.0	**HIGH** 2.0 x 5.0 = 10.0
	POSSIBLE (3.0)	**LOW** 3.0 x 1.0 = 3.0	**MEDIUM** 3.0 x 2.0 = 6.0	**MEDIUM** 3.0 x 3.0 = 9.0	**HIGH** 3.0 x 4.0 = 12.0	**HIGH** 3.0 x 5.0 = 15.0
	LIKELY (4.0)	**MEDIUM** 4.0 x 1.0 = 4.0	**MEDIUM** 4.0 x 2.0 = 8.0	**HIGH** 4.0 x 3.0 = 12.0	**HIGH** 4.0 x 4.0 = 16.0	**CRITICAL** 4.0 x 5.0 = 20.0
	CERTAIN (5.0)	**MEDIUM** 5.0 x 1.0 = 5.0	**HIGH** 5.0 x 2.0 = 10.0	**HIGH** 5.0 x 3.0 = 15.0	**CRITICAL** 5.0 x 4.0 = 20.0	**CRITICAL** 5.0 x 5.0 = 25.0

Risk Remediation

- As part of this risk remediation process, the Company shall determine objectives for mitigating or treating risks. All high and critical risks must be treated. For continuous improvement purposes, company managers may also opt to treat medium and/or low risks for company assets.
- Treatment options for risks include the following options:
  - Selection or development of security control(s).

    - Transferring the risks to a third party; for example, by purchasing an insurance policy or signing a contract with suppliers or partners.
    - Avoiding the risk by discontinuing the business activity that causes such risk.
    - Accepting the risk; this option is permitted only if the selection of other risk treatment options would cost more than the potential impact of the risk being realized.
- After selecting a treatment option, the risk owner should estimate the new impact and likelihood values after the planned controls are implemented.

Regular Reviews of Risk Assessment and Risk Treatment

- The Risk Assessment Report must be updated when newly identified risks are identified. At a minimum, this update and review shall be conducted once per year.

Reporting

- The results of risk assessments, and all subsequent reviews, shall be documented in a Risk Assessment Report.

Software Development Life Cycle Policy

SOC 2 Criteria: CC8.1

Keywords: Change management, OWASP, Software lifecycle

Purpose

This policy defines the high-level requirements for providing business program managers, business project managers, technical project managers, and other program and project stakeholders guidance to support the approval, planning, and life-cycle development of Cycom Data Systems software systems.

Policy

Cycom Data Systems must establish and maintain processes for ensuring that its computer applications or systems follow an SDLC process which is consistent and repeatable.

Software Development Phases and Approach Standard

A Software Development Project consists of a defined set of phases:

Determine System Need Phase

The Determine System Need phase is the period of time in which an information system need is identified and the decision is made whether to commit the necessary resources to address the need.

Define System Requirements Phase

The Define System Requirements phase is the period in which the User Requirements are broken down into more detailed requirements which can be used during designing and coding.

Design System Component Phase

The Design System Components phase transforms requirements into specifications to guide the work of the Development phase. The decisions made in this phase address how the system will meet the functional, physical, interface, and data requirements. Design phase activities may be conducted in an iterative fashion, producing a system design that emphasizes the functional features of the system and technical detail.

Build System Component Phase

The Build phase transforms the detailed, system design into complete coded software units and eventually, into an integrated product for release. Each software unit and subsequent integrated units are tested thoroughly. System documents that support installation and operations are also developed in this phase.

Evaluate System Readiness Phase

This Evaluate phase is to ensure that the system as designed and built satisfies the requirements of the user. Whenever possible, independent testers measure the system's ability to perform the functions that are required by the customer and ensure an acceptable level of quality and performance. Once the phase is complete, it will be evident whether or not the system is ready for operation or redevelopment.

System Deployment Phase

System Deployment phase is the final phase of the development life cycle, when the system is released initially to a pilot site and then into the production environment. All necessary training for using the system is accomplished.

The sequence of the phases depends on the software development approach taken. These approaches include but are not limited to:

- Waterfall Development
- Agile Development
- Iterative Development
- Staged Delivery Development

Based on the approach for and the size of the software development, some of the phases can be combined. In Iterative Development there may be multiple Cycles (iterations) of the above phases before the final software is released.

SDLC Control Guidelines

The SDLC process will adhere to the following controls:

- Adequate procedures should be established to provide separation of duties in the origination and approval of source documents. This shall include but not be limited to separation of duties between Personnel assigned to the development/test environment and those assigned to the production environment.
- Modification of code or an emergency release will follow the change control standard.
- Secure programming standards should be followed. Secure code training should be provided to Cycom Data Systems's developers.
- All software deployed on Corporate or Hosted infrastructure must prevent security issues including but not limited to those covered by SAN and OWASP.
- Code changes are reviewed by individuals other than the originating code author and by individuals who are knowledgeable in code review techniques and secure coding practices.
- Overrides of edit checks, approvals, and changes to confirmed transactions should be appropriately authorized, documented, and reviewed.
- Application development activity should be separated from the production and test environments. The extent of separation, logical or physical, is recommended to be appropriate to the risk of the business application or be in line with customer contractual requirements. The level of separation that is necessary between production, development, and test environments should be evaluated and controls established to secure that separation.
- All changes to production environments should strictly follow change control procedures, including human approval of all changes, granted by an authorized owner of that environment. Automated updates should be disallowed without such approval.
- Active production environments should not be re-used as test environments. Inactive and/or decommissioned production environments should not be used as test environments unless all private data has been removed. Test environments should not be re-used as production environments without going through a decommissioning and recommissioning process that cleans all remnants of test data, tools, etc.
- Individuals who are responsible for supporting or writing code for an internet-facing application, or internal application that utilizes web technology and handles customer information, should complete **annual** security training specific to secure coding practices. For individuals supporting or writing code for an internet-facing application, training should also include topics specific to internet threats. The individual should complete the training prior to writing or supporting the code. The training must include OWASP secure development principles as well as OWASP top 10 vulnerability awareness for the most recent year available.
- Custom accounts and user IDs and/or passwords should be removed from applications before applications become active or are released to customers.
- Production data should not be used in testing or development environments.
- Security controls that are in place for the production copy in the test system should be production quality (e.g. mirroring the production controls over the data).
- When conducting quality assurance (QA) testing prior to the release of a new feature requiring user input where constraints on user input may be reasonably understood, feature acceptance tests must include testing of edge and boundary cases.

For situations demonstrating that testing needs to use production data, the requirements are the following:

- The Information Resource Owner will provide approval before production data can be used for testing purposes.
- Wherever possible, the production data should be tokenized or anonymized instead of using production data.
- Testing and parallel runs should use a separate copy of production data and the test location or destination should be acceptable (e.g. loading confidential production data to a laptop for testing is not acceptable).
- The data should not be extracted, handled, or used by the test process in a manner that subjects the data to unauthorized disclosure.
- The data should be accessed on a need-to-know basis.
- Normal test activities should not use production data. In cases where test activity requires access to production data, access to production data should be restricted to only those individuals who have a documented business need. Only the information with the documented business need should be accessible by those users.
- Production data used for testing should be securely erased upon completion of testing.
- Test data and accounts will be removed before being placed into production.
- Restricted/Protected Information will be encrypted according to the Encryption Standard while at rest or in transit.
- Error messages must be handled securely and they must not leak sensitive information.

System Access Control Policy

SOC 2 Criteria: CC6.2, CC6.3, CC6.4, CC6.5, P4.3

Keywords: Access, Least privilege principle, Least access principle, Role change, Access reviews

---

Background

Access to Cycom Data Systems systems and applications is limited for all users, including but not limited to workforce members, volunteers, business associates, contracted providers, and consultants. Access by any other entity is allowable only on a minimum necessary basis. All users are responsible for reporting an incident of unauthorized use or access of the organization's information systems.

Purpose

The purpose of this procedure is to provide a policy and guideline for creating, modifying, or removing access to the company’s network and data by creating, changing or deleting the network account configuration for a User.

Scope

This policy and defined process is used to allow access to the company’s data and systems to individuals who meet the requirements defined in this policy. This policy governs individuals who are granted access that is necessary to support the business. This policy relates to all data used, processed, stored, maintained, or transmitted in and through the company’s systems.

Access Establishment and Modification

Requests for access to Cycom Data Systems Platform systems and applications are made formally using the following process:

1. A Cycom Data Systems workforce member initiates the access request by creating an Issue in the Cycom Data Systems ticketing system.
    1. User identities must be verified prior to granting access to new accounts.
    2. Identity verification must be done in person where possible; for remote employees, identities must be verified over the phone.
    3. For new accounts, the method used to verify the user's identity must be recorded on the Issue.
2. The Security Officer will grant or reject access to systems as dictated by the employee's job title. If additional access is required outside of the minimum necessary to perform job functions, the requester must include a description of why the additional access is required as part of the access request.
3. If the request is rejected, it goes back for further review and documentation.
4. If the review is approved, the request is marked as “Done”, and any pertinent notes are added.

Access Reviews

All access to Cycom Data Systems systems and services is reviewed and updated on annual basis to ensure proper authorizations are in place commensurate with job functions. The process for conducting reviews is outlined below:

1. The Security Officer initiates the review of user access by creating an Issue in the Cycom Data Systems Ticketing System
2. The Security Officer is assigned to review levels of access for each Cycom Data Systems workforce member.
3. If user access is found during review that is not in line with the least privilege principle, the Security Officer may modify user access and notify the user of access changes.
4. Once the review is complete, the Security Officer then marks the ticket as “Done”, adding any pertinent notes required.

Workforce Clearance

- The level of security assigned to a user to the organization's information systems is based on the minimum necessary amount of data access required to carry out legitimate job responsibilities assigned to a user's job classification.
- All access requests are treated on a **"least-access principle."**
- Cycom Data Systems maintains a minimum necessary approach to access to Customer data.

Unique User Identification

- Access to the Cycom Data Systems Platform systems and applications is controlled by requiring unique User Login IDs and passwords for each individual user and developer.
- Passwords requirements mandate strong password controls.
- Passwords are not displayed at any time and are not transmitted or stored in plain text.
- Default accounts on all production systems, including root, are disabled.
- Shared accounts are not allowed within Cycom Data Systems systems or networks.
- Automated log-on configurations other than the company’s approved Password Management provider that store user passwords or bypass password entry are not permitted for use with Cycom Data Systems workstations or production systems.

Automatic Logoff

- Users are required to make information systems inaccessible by any other individual when unattended by the users (ex. by using a password protected screen saver or logging off the system).

Employee Workstation Use

All workstations at Cycom Data Systems are company owned, and all are laptop products running Windows, Mac OSX or Linux.

- Workstations may not be used to engage in any activity that is illegal or is in violation of organization's policies.
- Access may not be used for transmitting, retrieving, or storage of any communications of a discriminatory or harassing nature or materials that are obscene or "X-rated". Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference, or health condition shall be transmitted or maintained. No abusive, hostile, profane, or offensive language is to be transmitted through the organization's system.
- Information systems/applications also may not be used for any other purpose that is illegal, unethical, or against company policies or contrary to organization's best interests. Messages containing information related to a lawsuit or investigation may not be sent without prior approval.
- Solicitation of non-company business, or any use of organization's information systems/applications for personal gain is prohibited.
- Users may not misrepresent, obscure, suppress, or replace another user's identity in transmitted or stored messages.
- Workstation hard drives must be encrypted
- All workstations have firewalls enabled to prevent unauthorized access unless explicitly granted.

Employee Termination/Offboarding Procedures

1. The Human Resources Department (or other designated department), users, and their supervisors are required to notify the Security Officer upon completion and/or termination of access needs and facilitate completion of the "Termination Checklist".
2. The Human Resources Department, users, and supervisors are required to notify the Security Officer to terminate a user's access rights if there is evidence or reason to believe the following (these incidents are also reported on an incident report and is filed with the Privacy Officer):
    1. The user has been using their access rights inappropriately;
    2. A user's password has been compromised (a new password may be provided to the user if the user is not identified as the individual compromising the original password);
3. The Security Officer will terminate users' access rights within 1 business day of termination/separation, and will coordinate with the appropriate Cycom Data Systems employees to terminate access to any non-production systems managed by those employees.
4. The Security Officer audits and may terminate access of users that have not logged into the organization's information systems/applications for an extended period of time.

Vendor Management Policy

SOC 2 Criteria: CC2.3, CC3.2, CC3.3, CC3.4, CC4.1, CC4.2, CC6.4, CC9.2, P6.2, P6.4

Keywords: Vendors, SOC report review, 3rd party applications, Vendor contracts

---

Purpose

The purpose of this policy is to establish requirements for ensuring third-party service providers/vendors meet Cycom Data Systems requirements for preserving and protecting Cycom Data Systems Data.

Scope

The policy applies to all IT vendors and partners who have the ability to impact the confidentiality, integrity, and availability of Cycom Data Systems's technology and sensitive information, or who are within the scope of Cycom Data Systems's information security program. This policy also applies to all employees and contractors that are responsible for the management and oversight of IT vendors and partners of Cycom Data Systems.

Background

The overall security of Cycom Data Systems is highly dependent on the security of its contractual relationships with its suppliers, vendors, and partners. This policy defines requirements for effective management and oversight of such suppliers, vendors, and partners from an information security perspective. The policy prescribes minimum standards a vendor must meet from an information security standpoint, including security clauses, risk assessments, service level agreements, and incident management.

Policy

Cycom Data Systems makes every effort to assure all 3rd party organizations are compliant and do not compromise the integrity, security, and privacy of Cycom Data Systems or Cycom Data Systems Customer data. 3rd Parties include Customers, Partners, Subcontractors, and Contracted Developers.

- IT vendors are prohibited from accessing Cycom Data Systems's information security assets until a contract containing security controls is agreed to and signed by the appropriate parties.
- All IT vendors must comply with the security policies defined and derived from the Information Security Policy.
- IT vendors and partners must ensure that organizational records are protected, safeguarded, and disposed of securely. Cycom Data Systems strictly adheres to all applicable legal, regulatory and contractual requirements regarding the collection, processing, and transmission of sensitive data such as Personally-Identifiable Information (PII).
- Cycom Data Systems may choose to audit IT vendors and partners to ensure compliance with applicable security policies, as well as legal, regulatory and contractual obligations.

Vendor Inventory

An inventory of third party service providers shall be maintained, and the inventory shall include:

- Vendor risk level
- Types of data shared with the third party
- Brief description of services
- Main point of contact at the third party
- How access is granted to the third party vendor
- Significant controls in place
- Security report and/or questionnaire

Vendor risk level assessment will be based on the following considerations:

- **High**: the vendor stores or has access to sensitive data and a failure of this vendor would have critical impact on your business
- **Moderate:** the vendor does not store or have access to sensitive data and a failure of this vendor would not have critical impact on your business
- **Low:** the vendor doesn't store or have access to any data and a failure of this vendor would have very little to no impact on your business

Vendor Contracts

Formal contracts that address relevant security and privacy requirements must be in place for all third parties that process, store, or transmit confidential data or provide critical services. The following must be included in all such contracts:

- Contracts will acknowledge that the third party is responsible for the security of the institution's confidential data that it possesses, stores, processes, or transmits;
- Contracts stipulate that the third-party security controls are regularly reviewed and validated by an independent party;
- Contracts identify the recourse available to Cycom Data Systems should the third party fail to meet defined security requirements;

- Contracts establish responsibilities for responding to direct and indirect security incidents including timing as defined by service-level agreements (SLAs);
- Contracts specify the security requirements for the return or destruction of data upon contract termination;
- Responsibilities for managing devices (e.g., firewalls, routers) that secure connections with third parties are formally documented in the contract: and
- Contracts stipulate geographic limits on where data can be stored or transmitted.

Vulnerability Management Policy

SOC 2 Criteria: CC1.2, CC3.1, CC3.3, CC3.4, CC4.1, CC4.2, CC5.1, CC5.2, CC7.1, CC7.2

Keywords: Penetration testing, Pen testing, Vulnerability scans, Vulnerability priority levels, Security SLAs

---

Purpose

Cycom Data Systems policy requires that:

- All product systems must be scanned for vulnerabilities at least annually.
- All vulnerability findings must be reported, tagged, and tracked to resolution in accordance with the SLAs defined herein. Records of findings must be retained for at least 5 years.

Policy

Vulnerability Scanning and Infrastructure Security Testing

The scanning and identification of Cycom Data Systems's system vulnerabilities is performed by:

- Automated Drata security agent installed on all employees' machines.
- Azure Security Center

Penetration Testing

Penetration testing is performed regularly by either a certified penetration tester on Cycom Data Systems's security team or an independent third party.

Findings from a vulnerability scan and/or penetration test are analyzed by the Security Officer, together with IT and Engineering as needed, and reported through the process defined in the next section.

Security Findings Reporting, Tracking and Remediation

Cycom Data Systems follows a simple vulnerability tracking process using Jira. The records of findings are retained for 5 years.

Reporting a Finding

- Upon identification of a vulnerability (including vulnerability in software, system, or process), a Jira ticket is created.
- The description of the Finding should include further details, without any confidential information, and a link to the source.
- The Finding will be given a priority level in Jira.

Priority/Severity Ratings and Service Level Agreements

In an effort to quickly remediate security vulnerabilities, the following timelines have been put in place to address vulnerabilities:

Priority Level	SLA	Definition	Examples
Critical	1 Day	Vulnerabilities that cause a privilege escalation on the platform from unprivileged to admin, allows remote code execution, financial theft, unauthorized access to/extraction of sensitive data, etc.	Vulnerabilities that result in Remote Code Execution such as Vertical Authentication bypass, SSRF, XXE, SQL Injection, User authentication bypass
High	3 Days	Vulnerabilities that affect the security of the platform including the processes it supports.	Lateral authentication bypass, Stored XSS, some CSRF depending on impact
Medium	7 Days	Vulnerabilities that affect multiple users, and require little or no user interaction to trigger	Reflective XSS, Direct object reference, URL Redirect, some CSRF depending on impact
Low	30 Days	Issues that affect singular users and require interaction or significant prerequisites (MitM) to trigger.	Common flaws, Debug information, Mixed Content

In the case a severity rating and/or priority level is updated after a vulnerability finding was originally created, the SLA is updated as follow:

- Priority upgrade: reset SLA from time of escalation
- Priority downgrade: SLA time remains the same from time of creation/identification of finding

Resolving a Finding

- The Finding should be assigned to the owner responsible for the system or software package.
- All findings should be addressed according to the established SLA.
- No software should be deployed to production with unresolved CRITICAL or HIGH findings, unless an Exception is in place (see below).
- A finding may be resolved by
    1. providing a valid fix/mitigation
    2. determining as a false positive
    3. documenting an approved exception

Closing a Finding

- The assignee should provide a valid resolution (see above) and add a comment to the finding.
- The finding should be re-assigned to the Reporter or a member of the security team for validation.
- Upon validation, the finding can be marked as Done (closed) by the Reporter.
- Before the finding can be marked as closed by the reporter, the fix must be deployed to a development environment and have a targeted release date for deploying to production noted on the ticket.

Exceptions

- An Exception may be requested when a viable or direct fix to a vulnerability is not available. For example, a version of the package that contains the fix is not supported on the particular operating system in use.
- An alternative solution (a.k.a. compensating control) must be in place to address the original vulnerability such that the risk is mitigated. The compensating control may be technical or a process or a combination of both.
- An Exception must be opened in the form of a Jira ticket
- The Exception Issue must reference the original Finding by adding an Issue Link to the Finding issue.
- Each Exception must be reviewed and approved by the Security Officer and the impacted asset owner.

[SIGNATURES ON NEXT PAGE]

City of Redondo Beach

_____
Signature

James A. Light
_____
Printed Name

Mayor
_____
Title

_____
Date

Cycom Data Systems, Inc.

_____
Signature

_____
Printed Name

_____
Title

_____
Date

ATTEST:

_____
Eleanor Manzano, City Clerk

APPROVAL AS TO FORM:

_____
Michael W. Webb, City Attorney