Together Software

TABLE OF CONTENTS

Acceptable Use Policy

Our customers trust us, and they expect us to protect the data and resources they've shared with us. Part of how we'll uphold that trust is through pre-established policies so we don't need to make key decisions in critical moments.

Below, we explain the sections of our acceptable use policy: what each protects against, why a customer may care, and why we think each is important. We don't mean for the Acceptable Use Policy to intimidate, but we do aim for it to be clear.

General Use and Ownership

This section explains policy around separating work activities from personal activities as much as possible. Understand that the systems you use for work, including a company-provided laptop, have a *much lower expectation of privacy* than systems you own. You may use your company devices for reasonable personal use, but those devices are not yours because:

- If the company is sued, all its devices are subject to discovery, which means opposing counsel will have access to your data.
- When we troubleshoot our systems, company administrators may have access to your data.
- We may terminate an employee, which may include giving another employee access to the terminated employees' devices and accounts.
- If we are breached, outside investigators will likely inspect all use of an account and/or device, no matter its purpose.

Please limit personal use of company-provided devices as much as possible and remember that corporate devices are not your personal property. Our policies are strict so that we do not have to make judgment calls on a case-by-case basis in high-stress situations.

Security and Proprietary Information

This section describes behaviors the company expects of you, including password hygiene and the use of multi-factor authentication.

Acceptable Use

The first part of this section details the consequences for malicious, negligent, and/or delinquent behavior. Neither intentionally harm others nor break laws.

The section's second part emphasizes that your employment by the company does not make you one of the company's public representatives. Instead, public communication and brand are

controlled centrally at the company. While email and social media are mentioned specifically, please be conservative overall in how you represent yourself as an employee.

Policy Compliance

This section details the information security team's role in measuring, enforcing, and making exceptions to the policy and the potential consequences, including termination, for policy violations.

Acceptable Use Policy

1. Overview

Together Software's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Together Software's established culture of openness, trust and integrity. Instead, the team is committed to protecting Together Software's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Together Software. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is an organizational effort involving the participation and support of every employee and affiliate who deals with Together Software information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Together Software. These rules are in place to protect the employee and Together Software. Inappropriate use exposes Together Software to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct business or interact with internal networks and business systems, whether owned or leased by Together Software, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at Together Software, including Together Software-affiliated personnel employed with third parties. This policy applies to all equipment that is owned or leased by Together Software.

4. Policy

4.1 General Use and Ownership

4.1.1 Proprietary information stored on electronic and computing devices whether owned or leased by Together Software, the employee or a third party, remains the sole property of Together Software. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Policy.

4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of proprietary information.

4.1.3 You may access, use or share proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within Together Software may monitor equipment, systems and network traffic at any time, per the company's auditing practices, details of which are documented in relevant technology and security-related policies.

4.1.6 Together Software reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the Asset Management Policies.

4.2.2 Providing access to another individual, either deliberately or through failure to secure access, is prohibited. In the event that such access is provided, either intentionally or inadvertently, it must be reported immediately to the IT security team.

4.2.3 Postings by employees from an email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Together Software, unless posting is in the course of business duties.

4.2.4 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware. If an employee suspects that they have inadvertently opened a malicious attachment, it must be reported immediately to the IT security team.

4.2.5 Employees must use multi-factor authentication to authenticate to corporate accounts whenever available.

4.2.6 Employees must use a password manager from the list of approved password managers to avoid insecure or shared passwords with accounts.

4.2.7 Employees must encrypt their devices if asked, and must not interfere or otherwise reduce the level of encryption on their devices.

4.2.8 Employees must install OS updates onto their devices if asked or prompted. Employees should also be proactive about applying OS updates to their devices.

4.2.9 Employees must use antivirus software to protect the integrity and confidentiality of their laptops if asked, and must not interfere or otherwise prohibit antivirus activities on their devices.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Together Software-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities: the following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the company.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes. Together Software Security team members providing pre-planned penetration testing and vulnerability scans on corporate networks, infrastructure and end user devices are exempt from this due to the nature of their job duties.
10. Port scanning or security scanning is expressly prohibited unless the Security team is notified in advance. Together Software Security team members providing pre-planned penetration testing and vulnerability scans on corporate networks, infrastructure and end user devices are exempt from this due to the nature of their job duties.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty. Together Software Security team members providing pre-planned penetration testing and vulnerability scans on corporate networks, infrastructure and end user devices are exempt from this due to the nature of their job duties.

12. Circumventing user authentication or security of any host, network or account. Together Software Security team members providing pre-planned penetration testing and vulnerability scans on corporate networks, infrastructure and end user devices are exempt from this due to the nature of their job duties.
13. Introducing honeypots, honeynets, or similar technology on the network.
14. Interfering with or denying service to any user other than the employee's host (for example, distributed denial of service (DDoS) attack).
15. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
16. Providing information about, or lists of, employees to parties outside Together Software.

4.3.2 Email and Communication Activities: When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company." Questions may be addressed to Together Software management.

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Posting the same or similar non-business-related messages to large numbers of newsgroups or mailing lists (newsgroup spam).
7. Use of unsolicited email originating from within Together Software's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by or connected via Together Software's network.

4.3.3 Blogging and Social Media

1. Blogging by employees, whether using Together Software's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Together Software's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Together Software's policy, is not detrimental to Together Software's best interests, and does not interfere with an employee's regular work duties. Blogging from Together Software's systems is also subject to monitoring.
2. Employees are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered by Together Software's Data Protection policy when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Together Software and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Together Software's Code of Conduct.
4. Employees may also not attribute personal statements, opinions or beliefs to Together Software when engaged in blogging or on any social media platforms, including but not emphasizing professional networks such as LinkedIn. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Together Software. Employees assume any and all risk associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Together Software 's trademarks, logos and any other intellectual property may also not be used in connection with any blogging activity.

5. Policy Compliance

5.1 Compliance Measurement

The Security Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Security Team in advance, and if applicable, documented in the Together Software Risk Register.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

- Asset Management Policy - Endpoints
- Data Protection Policy
- Information Security Policy
- Password Policy
- Responsible Disclosure Policy
- System Access Policy
- Code of Conduct

7. Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at https://www.sans.org/security-resources/glossary-of-terms/

- Blogging
- Honeypot
- Honeynet
- Proprietary Information
- Spam

Responsibility

The Security Team is responsible for ensuring this policy is followed.

Last updated: September 20, 2022

Artificial Intelligence (AI) Policy

This policy outlines the responsible use of Artificial Intelligence (AI) by employees at Together and the integration of AI functionalities within Together's application.

Employee use of AI

1. **Permitted Use**
   All employees are authorized to use AI tools to enhance productivity and decision-making.

2. **Compliance with Regulations**
   Employees must adhere to all relevant laws and internal policies when using AI.

3. **Data Protection**
   Under no circumstances should employees use AI to process or disclose Personally Identifiable Information (PII) without proper authorization and safeguards. Customer data should not be submitted into an AI tool.

4. **Ethical Use**
   AI should be used ethically, respecting privacy, non-discrimination, and fairness.

5. **Reporting Misuse**
   Any misuse or unethical application of AI must be immediately reported to the management.

AI Features in the Together Application

1. **Voluntary Use**
   Together Software **guarantees** that every AI feature integrated into the application will be non-mandatory, offering users the choice to opt-in or opt-out.

2. **Transparency**
   AI features will be clearly labelled, and their purpose and functioning will be transparent to users.

3. **Data Privacy**
   AI functionalities in the app will comply with the highest standards of data privacy and security.

4. **Continuous Improvement**
   AI features will be regularly evaluated and updated for effectiveness, fairness, and user satisfaction.

5. **User Feedback**
   User feedback on AI features will be actively sought and used to guide further improvements.

Policy Review and Updates

This policy is subject to periodic review and amendments to stay aligned with technological advancements and regulatory changes.

Disciplinary Process

Violation of this policy will result in disciplinary action, up to and including termination of employment.

Asset management policy

Introduction

This Asset Management Policy is designed to protect customers' data stored on endpoints, including laptops and mobile devices. It details how Together accounts for endpoint information technology assets (e.g. employee computers) and outlines what should be done if assets are lost, destroyed, or otherwise damaged.

Asset Standards

The Security team must review and approve any new type of asset (e.g. a new computer model) that will be used for Together's operations.

Currently, approved device manufacturer(s) include Apple. Devices should be configured such that there's reasonable confidence they will last 36 months.

Configuration Standards

When Together purchases the same hardware asset repeatedly, the team should design and implement consistent, secure configuration standards to ensure assets are configured securely and identically. The standards should be based on the team and role of the Together employee who will be using the asset.

All devices provided by the company should enforce via device management the baseline configuration:

- Password management software
- Hard disk encryption (e.g. FileVault) enabled
- Password-protected screensaver that activates automatically after 15 minutes or less
- Personal firewall (e.g. OS X's application firewall) enabled
- Data cannot be transferred to removable media
- Data cannot be transferred over bluetooth

Variations to the Configuration Standard

Deviations from the standard configuration should be documented and approved by the Together Security team. The Security team should only approve deviations for which there's a valid business need. Deviations will be documented in the company's inventory list.

Support of Non-Standard Assets

"Non-standard assets" are those that don't conform to Together's asset and/or configuration standards. Together does not permit Non-standard assets to access Together's network.

Bring Your Own Device (BYOD) Policy

Together provides all employees with devices that conform to this policy. Together does not permit employees to access company information using their own devices with the exception of using mobile devices for a limited functionality. All employee-owned mobile devices must conform to Together security policies if they're used to access Together data, systems, and/or IT infrastructure.

Every employee who chooses to use their personal mobile device for work purposes must ensure the device supports MDM (mobile device management) and must adhere to the Mobile Device Policy section outlined in the Information Security Policy.

Asset Procurement Guidelines

Any request for Asset Procurement must be reviewed for compliance with Together's Asset Standards by the Together Security team. Once the request passes review, the Together Security team is responsible for

placing orders to procure the requested assets. Software Licensing Guidelines Together's Vendor Management Policy details the policies for third-party software and services.

Technical Support and Maintenance Practices

The Together Security team is responsible for technical support. The Security team handles device maintenance. Support and maintenance requests should conform with all of Together's security policies. Company maintenance policies are:

- If a device breaks in the first 36 months, the employee will be given a loaner device while the original is repaired
- If an employee leaves the company, his/her device(s) will be wiped and reissued if purchased in the past 18 months; older devices will be added to the loaner pool
- Computers may be replaced when they are 36 months old

The Security team should handle device exceptions that do not meet these policies.

Configuration Management Guidelines

Security team is responsible for installing critical firmware and software updates on the assets they use exclusively. The Security team is responsible for installing firmware and software updates on communal assets (e.g. desktops and/or large monitors).

Asset Inventory Practices

The Together Security team is tasked with maintaining a list of all company-owned assets. Employees must immediately report lost, stolen, or damaged devices to the Together Security team, which will then remotely lock down the missing asset as soon as possible.

Asset Disposal Guidelines

Whenever possible, Together refurbishes and reissues assets. If an asset will not be reused internally, the Together Security team must reformat the hard drive to delete customer data and invalidate access credentials before disposing of it.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Together management will determine how serious an employee's offense is and take the appropriate action.

Responsibility

The Security team is responsible for ensuring this policy is followed.

Last updated: January 10, 2024

Backup Policy

Together Software (US)'s Backup Policy describes how often service and customer data is backed up. All original (non-derived) customer data on infrastructure operated by Together Software (US) should be backed up.

Timing

Together Software (US) configures full, daily database backups of all critical data stored in our operational database. If a database instance is deleted, all associated backups are also automatically deleted.

Endpoint Backups

Together does not maintain backups of employee endpoints (laptops or computers). Key tools, documents, and work products are expected to be stored on cloud services and shared file drives, so creating and maintaining backups of employee endpoints is not necessary.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Together Software (US) management will determine how serious an employee's offense is and take the appropriate action.

Responsibility

The Security Team is responsible for ensuring this policy is followed.

Last updated: September 20, 2022

Business Continuity Policy

The following consists of a general Business Continuity Policy that represents governance of contingency plans for certain business-impacting outages and vendor disruption of service.

Business Continuity Policies

- Together Software performs testing of this Business Continuity Plan on a semi-annual basis. The Security Team is responsible for coordinating and conducting a semi-annual rehearsal of this Business Continuity Plan.
- Whenever the BCP is enacted, it must be followed up with a retrospective in order to identify lessons learned and playbooks needing creation.
- Business Impact Assessments (BIA's) need to be conducted upon onboarding new, business-critical vendors. Please see the Vendor Management policy for more information and instructions.

Together Software Business Continuity Plan

The following consists of a general Business Continuity Plan for Together Software that represent vendor and service outages that could affect Together Software business operations, including contingency plans and workarounds. More detailed playbooks are available in Disaster Recovery Plan for infrastructure disasters.

This plan identifies key resources and needs to ensure that business may continue, perhaps in a limited capacity, in the event of a disaster.

The plan includes information such as key suppliers, contingency plans and alternative business location.

Alternate Business Location

If Together Software's primary work site is unavailable, personnel will work from home.

Key Vendors - Contacts and Contingency Plans

Communications, Collaboration & SSO

Employees at Together Software communicate with customers over email and are equipped to engage customers in video conferences or telephone calls. Together Software uses a Single Sign-On (SSO) provider for a number of business applications.

If an outage is suspected with one of these systems, visit that system's status page. If no listed issue would explain the observed outage, submit a support ticket to the service provider through their support page.

Customer Support - Zendesk

Customer Support functions for Together Software are supported via the third-party tool Zendesk.

If an outage is suspected, visit the Zendesk status page at the tool's publicly-available status page to see if there is a known issue. If no issue is found, submit a support ticket to Zendesk. If there is no resolution time horizon, ask the Security Team for access to the shared support@togetherplatform.com inbox to reply to support emails from your own email client.

Business Continuity Procedures by Scenario

Email provider outage

1. Customer Support communication is still maintained using third party tool Zendesk
2. Contact provider for remediation timeline estimates. In case remediation timeline estimates are not acceptable switch to another provider

Infrastructure provider outage

1. Update publicly-available status page with the outage information
2. Contact provider for remediation timeline estimates. In case remediation timeline estimates are not acceptable act according to disaster recovery plan

SSO provider outage

1. Continue using service that provide alternative authorization methods
2. Contact provider for remediation timeline estimates. In case remediation timeline estimates are not acceptable switch to another provider

Domain provider outage

In case end users are affected and outage is causing major infrastructure issues

1. Update publicly-available status page with the outage information
2. Contact provider for remediation timeline estimates. In case remediation timeline estimates are not acceptable act according to disaster recovery plan

In case end users are not affected and outage is causing minor infrastructure issues

1. Contact provider for remediation timeline estimates. In case remediation timeline estimates are not acceptable switch to another provider

Responsibility

The Together Software Security team is responsible for ensuring this policy is followed.

Appendix A: Insurance

Together Software is covered by Technology Errors and Omissions and Cyber Liability insurance through Everspan Indemnity Insurance Company, under policy number EM3EII-AX-000259-01, to protect against disruptions or disasters.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Together Software management will determine how serious an employee's offense is and take the appropriate action.

Last updated: February 13th, 2024

Change Management Process and Standard - Code Deployments

Together Software (US)'s Change Management Policy describes how changes to the Together Software (US) system is proposed, reviewed, deployed, and managed. This policy covers all changes made to the Together Software (US) software, regardless of their size, scope, or potential impact.

This policy is designed to mitigate the risks of:

- corrupted or destroyed information
- degraded or disrupted computer performance
- productivity losses
- introduction of new vulnerabilities, configuration errors and software bugs in infrastructure and code
- exposure to reputation risk

Version Control

All of our software is version controlled and synced between contributors (developers). Access to the central repository is restricted based on an employee's role.

Using a decentralized version control system allows multiple developers to work simultaneously on features, bug fixes, and new releases; it also allows each developer to work on their own local code branches in a local environment.

All code is written, tested, and saved in a local repository before being synced to the origin repository. Writing code locally decouples the developer from the production version of our code base and insulates us from accidental code changes that could affect our users. In addition, any changes involving the persistence layer (database) are performed locally when developing new code, where errors or bugs can be spotted before the change is deployed to users.

Branching Model

Production branch

The **production** branch reflects the current state of the application in production.

Feature branches

We operate on a continuous delivery model, such that there is no single staging branch through which merges into **production** are made. Releases are not scheduled, they can happen any time features are ready for release by a developer.

Feature branches are used to develop new features for a future release. A given feature branch

will exist as long as the feature is in development; the branch will be deployed to a 'production-like' staging environment, to be tested, before being merged into the **production** branch with a pull request. The branch may also be discarded (if the feature will not be added to an upcoming release).

Feature branches must run through the entire set of continuous integration tests before being merged into **production**.

Security bugs

Together Software (US) recognizes that security bugs represent key issues that should be resolved quickly to maintain the security, confidentiality, privacy, processing integrity, and availability of the service. Together Software (US) commits to resolving security bugs within reasonable timelines as outlined by company procedural commitments in Vanta.

Hotfix branches

Because we operate on a continuous delivery model, there is no practical difference between a hotfix branch and a regular feature release. Both merge into production and both must pass all deployment checks and test suites for a pull request to be mergable.

Change Initiation

To initiate a change, the developer first creates a feature branch on his or her local machine. Code changes are grouped into diffs, each of which represents a proposed change to the codebase.

Pull Requests

When a developer finishes a feature branch, they make a pull request to merge those changes into production. This submits the changes for peer review. For all code changes, the reviewer should be different from the author.

Pull requests allow developers to describe the changes they're making; co-workers can review the set of changes in a code review. Pull requests also trigger automated testing and code-quality checks that must be completed and returned successfully before merging is allowed. Testing and approval are logged by the system.

A pull request's details section should be used to note any non-code changes (e.g. environment or database changes) needed before the commits are merged.

Once tests pass and the code is approved, the author can merge the code to the central repository.

Merging a Pull Request

Before merging a pull request, the developer should check that all prerequisites have been met, including environment changes or database migrations. Once non-code changes have been implemented, the pull request can be merged.

If the application is deployed through our standard, zero-downtime development process, the developer's job is complete.

If any of these changes necessitate system down-time, the merge should take place within a scheduled and pre-announced window when customers are less likely to be affected.

Code Reviews, Change Review, and Change Approval

Before a feature branch is merged, a code review should be performed. Code reviews are

performed by a second developer (i.e. not the one who wrote the code), who considers questions like:

- Are there any obvious logic errors in the code?
- Are all cases specified in the requirements fully implemented?
- Is there sufficient automated testing for the new code? Do existing automated tests need to be rewritten to account for code changes?
- Does the new code conform to existing style guidelines?
- Are there any egregious security errors as defined by the *OWASP Top 10*?

A code review should take place after all code has been written and automated tests have been run and passed, as this ensures the reviewer's time is spent checking what automation misses.

The reviewer should note all potential issues with the code; it is the responsibility of the author(s) to address those issues or explain why they are not applicable.

Once the review process finishes, each reviewer should leave a comment on the pull request confirming the change is accepted and approve the entire pull request. Only when the pull request is accepted may the original author(s) may merge their change into the release branch.

Automated Testing

When a pull request is initiated, our automated test suite is triggered to run against the new code.

Deployment

The system is monitored on a continuous basis. Should the site be negatively affected by a change, that code change is rolled back.

Zero Downtime Deployment

Zero-downtime deployments allow us to make changes without waiting for a change window and allow us to return the application to a previous state easily.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Together Software (US) management will determine how serious an employee's offense is and take the appropriate action.

Responsibility

The Security Team is responsible for ensuring this policy is followed.

Last updated: September 20, 2022

Code of Conduct

Purpose

The primary goal of Together Software's Code of Conduct is to foster inclusive, collaborative and safe working conditions for all Together Software staff. As such, Together Software are committed to providing a friendly, safe and welcoming environment for all staff, regardless of gender, sexual orientation, ability, ethnicity, socioeconomic status, and religion (or lack thereof).

This code of conduct outlines our expectations for all Together Software staff, as well as the consequences for unacceptable behavior.

Scope

The Code of Conduct applies to all Together Software staff. This includes full-time, part-time and contractor staff employed at every seniority level. The Code of Conduct is to be upheld during all professional functions and events, including but not limited to business hours at the Together Software office, during Together Software-related extracurricular activities and events, while attending conferences and other professional events on behalf of Together Software, and while working remotely and communicating on Together Software resources with other staff.

We expect all Together Software staff to abide by this Code of Conduct in all business matters -- online and in-person -- as well as in all one-on-one communications with customers and staff pertaining to Together Software business.

This Code of Conduct also applies to unacceptable behavior occurring outside the scope of business activities when such behavior has the potential to adversely affect the safety and well-being of Together Software staff and clients.

Culture & Citizenship

A supplemental goal of this Code of Conduct is to increase open citizenship by encouraging participants to recognize the relationships between our actions and their effects within Together Software culture.

Be welcoming. We strive to be a company that welcomes and supports people of all backgrounds and identities. This includes, but is not limited to members of any race, ethnicity, culture, national origin, color, immigration status, social and economic class, educational level, sexual orientation, gender identity and expression, age, size, family status, political belief, religion, and mental and physical ability.

Be considerate. Your work at Together Software will be used by other people, and you in turn will depend on the work of others. Any decision you take will affect users and colleagues, and you should take those consequences into account when making decisions.

Be respectful. Not all of us will agree all the time, but disagreement is no excuse for poor behavior and poor manners. We might all experience some frustration now and then, but we

cannot allow that frustration to turn into a personal attack. It's important to remember that a company where people feel uncomfortable or threatened is neither productive or pleasant. Together Software staff should always be respectful when dealing with other personnel as well as with people outside of Together Software employment.

Acceptable and Expected Behavior

The following behaviors are expected and requested of all Together Software staff:

- Participate in an authentic and active way. In doing so, you contribute to the health and longevity of Together Software.
- Exercise consideration and respect in your speech and actions at all times.
- Attempt collaboration before conflict.
- Refrain from demeaning, discriminatory, or harassing behavior and speech.
- Be mindful of your surroundings and of your fellow participants. Alert Together Software leaders if you notice a dangerous situation, someone in distress, or violations of this Code of Conduct, even if they seem inconsequential.
- Remember that Together Software events may be shared with members of the public and Together Software customers; please be respectful to all patrons of these locations at all times.

Unacceptable Behavior

The following behaviors are considered harassment and are unacceptable within our community:

- Violence, threats of violence or violent language directed against another person.
- Sexist, racist, homophobic, transphobic, ableist or otherwise discriminatory jokes and language.
- Posting or displaying sexually explicit or violent material.
- Posting or threatening to post other people's personally identifying information ("doxing").
- Personal insults, particularly those related to gender, sexual orientation, race, religion, or disability.
- Inappropriate photography or recording.
- Inappropriate physical contact. You should have someone's consent before touching them in any manner.
- Unwelcome sexual attention. This includes sexualized comments or jokes; inappropriate touching, groping, and unwelcome sexual advances.
- Deliberate intimidation, stalking or following (online or in person).
- Advocating for, or encouraging, any of the above behavior.
- Repeated harassment of others. In general, if someone asks you to stop, then stop.
- Other conduct which could reasonably be considered inappropriate in a professional setting.

Weapons Policy

No weapons will be allowed at Together Software events, office locations, or in other spaces covered by the scope of this Code of Conduct. Weapons include but are not limited to guns, explosives (including fireworks), and large knives such as those used for hunting or display, as well as any other item used for the purpose of causing injury or harm to others.

Anyone seen in possession of one of these items will be asked to leave immediately and will be subject to punitive action up to and including termination and involvement of law enforcement authorities. Together Software staff are further expected to comply with all state and local laws on this matter.

Consequences of Unacceptable Behavior

Unacceptable behavior from any Together Software staff, including those with decision-making authority, will not be tolerated.

Anyone asked to stop unacceptable behavior is expected to comply immediately.

If a staff member engages in unacceptable behavior, Together Software leadership may take any action deemed appropriate, up to and including suspension or termination.

Reporting Violations

If you are subject to or witness unacceptable behavior, or have any other concerns, please notify an appropriate member of Together Software leadership as soon as possible.

It is a violation of this policy to retaliate against any person making a complaint of Unacceptable Behavior or against any person participating in the investigation of (including testifying as a witness to) any such allegation. Any retaliation or intimidation may be subject to punitive action up to and including termination.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Together Software management will determine how serious an employee's offense is and take the appropriate action.

Responsibility

It is the CEO's responsibility to ensure this policy is followed.

Last updated: September 20, 2022

Encryption & Key Management Policy

This policy provides guidance to limit encryption to those algorithms that have received substantial public review and have been proven to work effectively.

Additionally, this policy document provides Together Software (US) encryption standards and best practices to ensure that Together Software (US) consistently follows industry standards for Encryption and Key Management.

This policy and standard apply to all Together Software (US) employees, contractors, and third-party vendors when sensitive data, such as customer data, Together Software (US) secrets and PII, are in scope.

Data Encryption Policy

- All sensitive data in transit and at rest must be encrypted using strong, industry-recognized algorithms.
- Together Software (US) maintains approved encryption algorithm standards. These internal standards are reviewed and subject to change when significant changes to encryption standards within the security industry change.
- Together Software (US) will not engage in "roll-your-own" encryption, algorithms, or practices and will not use "security through obscurity" within production infrastructure or applications.
- All Together Software (US)-owned, employee-utilized computers are to have full disk encryption enabled at all times, as these devices are expected to interact with Together Software (US) resources, infrastructure and/or client data while performing Together Software (US) business.
- All Together Software (US)-owned wireless networks, including both corporate and guest networks, are to encrypt corporate office data in transit using WPA2-AES encryption.

Data in Transit

- The minimum acceptable TLS standard in use by the company is 1.2
- All Together Software (US) public web properties, applicable infrastructure components and applications using SSL/TLS, IPSEC and SSH to facilitate the encryption of data in transit over open, public networks, must have certificates signed by a known, trusted provider.

GCP Data Encryption

Together uses GCP resources to store and encrypt sensitive data. All GCP resources are encrypted at rest by default, using Google-managed keys. GCP server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256) or 128-bit Advanced Encryption Standard (AES-128), to encrypt Together data.

Together Software (US) Encryption Standards

The Security Team is responsible for reviewing all encryption algorithms in use. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the *IETF/IRTF Cipher Catalog*, or the set defined for use in the United States National Institute of Standards and Technology *(NIST) publication FIPS 140-2* , or any superseding documents according to the date of implementation.

Algorithms in use must meet the standards defined for use in *NIST publication FIPS 140-2* or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

Together Software (US) Encryption Key Creation & Storage Standards

Encryption Keys generated, stored, and managed by Together Software (US)

- Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.
- Key generation must be seeded from an industry standard random number generator (RNG). For examples, see *NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2*.

Auditing

The Security Team will verify compliance to this policy through various methods, including but not limited to code reviews, periodic infrastructure and database reviews, Vanta platform monitoring, and internal and external audits. Feedback will be provided to the appropriate Together Software (US) team(s) upon completion of audits and reviews if remediation is required.

Exceptions

Any exception to the policy must be approved by the Security Team in advance and placed on a risk register for monitoring and periodic review.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including employment termination.

Responsibility

The Security Team is responsible for ensuring this policy is followed.

Last updated: August 10, 2022

Data Classification Policy

In order to effectively secure Together Software's data, staff must have a shared vocabulary to describe the data and the corresponding protection it requires. This policy describes how company data is classified and the levels of protection required for each classification.

Data Classification Standards

All Together Software information and all information entrusted to Together Software from third parties falls into one of four classifications, in order of increasing sensitivity.

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for Together Software.	• Press releases • Public website
Internal	Access to internal information is approved by management and is protected from external access.	• Internal memos • Design documents • Product specifications • Correspondences
Customer confidential	Information received from customers for processing or storage by Together Software. Together Software must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Customer operating data • Customer PII • Customers' customers' PII • Anything subject to a confidentiality agreement with a customer
Company confidential	Information collected and used by Together Software to operate the business. Together Software must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Legal documents • Contractual agreements • Employee PII • Employee salaries

Public

Public data is information that may be disclosed to any person regardless of their affiliation with Together Software. The "public" classification is not limited to data that is of public interest or intended to be distributed to the public; the classification applies to any data that does not

require any level of protection from disclosure.

While it might be necessary to protect original (source) documents from unauthorized modification, public data may be shared with a broad audience both within and outside Together Software, and no steps need be taken to prevent its distribution.

Internal

Internal data is information that is potentially sensitive and should not be shared with the public. Internal data generally should not be disclosed outside of Together Software without the permission of Together Software management. It is the responsibility of the data owner to designate information as internal where appropriate.

Unauthorized access has the potential to influence Together Software's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence.

Customer confidential

Customer-confidential data is information that, if made available to unauthorized parties, may adversely affect Together Software customers. This classification also includes data that Together Software is required to keep confidential, either by law or under a confidentiality agreement with non-customer third parties, such as vendors. This information is to be protected against unauthorized disclosure or modification. Customer-confidential data should be used only when necessary for business purposes with the permission of the customer and should be protected both when it is in use and when it is being stored, processed, or transmitted.

Unauthorized access has the potential to influence Together Software's operational effectiveness, violate contractual confidentiality agreements, initiate a security incident, or cause a major drop in both customer and industry confidence.

Company confidential

Company-confidential data is information that, if made available to unauthorized parties, might adversely affect Together Software. This information is to be protected against unauthorized disclosure or modification, and might be limited to executives, HR, and legal parties employed by or under contract with Together Software. Company-confidential data should be used only by pre-authorized parties and should be protected both when it is in use and when it is being stored, processed, or transmitted. Unauthorized access has the potential to influence Together Software's operational effectiveness, violate contractual confidentiality agreements, initiate a security incident, or cause a major drop in employee, customer, and industry confidence.

Scope

This data classification standard and policy is to be applied to all Together Software data, both physical and electronic. No data item is too small to be classified.

Policy

- Together Software managers or information owners shall be responsible for assigning classifications to information assets according to Together Software Data Classification Standards.
- Whenever possible, clearly label each piece of information with its data classification.
- All Together Software staff shall be guided by the information category in their handling of all Together Software information.

Non-Compliance

Since classifying data is an important part of protecting data and systems for Together Software, employees who purposely violate this policy are subject to disciplinary action up to and including denial of access, legal penalties, and/or dismissal. Any employee aware of any violation of this policy is required to report it to their supervisor or other authorized representative.

Responsibility

The Security team is responsible for communicating and upholding the Data Classification Policy and Standards.

All staff are responsible for following the Data Classification Policy and Standards.

Last updated: September 22, 2022

Data Deletion Policy

Together Software's Data Deletion Policy describes how customer data is deleted in connection with the cancellation or termination of a Together Software account.

This policy applies to all data collected by Together Software except:

- data that resides in third-party services managed and hosted by third parties, with the exception of the company's infrastructure provider
- data that resides in Together Software products or services that are in beta, testing, or an early access program

By default, a customer's data is stored for the duration of his or her contract with Together Software.

Together may delete customer data within 120 days following contract termination, with the exception of data that is required to establish proof of a right or a contract, which will be stored for the duration provided by enforceable law.

Once deleted, a customer's data is irretrievable. It's advised to export your data prior to contract termination. Should you require data retention beyond the standard 120 days, inform a Together Software representative about a legal hold within 7 days prior to termination.

Only the following employees can delete customer data in the event that Together Software is required to do so:

- Security engineer
- Support engineer

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Together Software management will determine how serious an employee's offense is and take the appropriate action.

Responsibility

It is the responsibility of the Security team to manage the list of team members that may handle customer requests for data deletion.

The Security team is responsible for ensuring this policy is followed.

Last updated: January 25, 2024

Data Protection Policy

Introduction

This policy refers to all data collected from employees, candidates, users, customers, vendors, or other parties that provide information to Together Software.

Together Software employees must follow this policy. Contractors, consultants, partners and any other external entities are also covered. Generally, our policy refers to anyone we collaborate with or who acts on our behalf and may need access to Together Software data.

Data Protection Policy

As part of our operations, we obtain and process information, some of which can be used to identify individuals (personally-identifiable information, or PII).

Our company collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

The data will be:

- Accurate and kept up-to-date
- Collected fairly and for lawful purposes only
- Processed by the company within its legal and ethical boundaries
- Protected against any unauthorized or illegal access by internal and external parties

The data will not be:

- Communicated informally
- Stored for more than the amount of time specified in our Terms of Service, Privacy Policy, customer contracts, or other binding agreements
- Downloaded to unapproved devices
- Transferred to organizations, states, or countries that do not have adequate data protection policies
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

In addition to ways of handling the data, Together Software has direct obligations towards people to whom the data belongs. Specifically we must:

- Let people know which of their data is collected
- Inform people about how we'll process their data
- Inform people about who has access to their information
- Have provisions in cases of lost, corrupted, or compromised data
- Allow people to request that we modify, erase, reduce, or correct data contained in our databases within legal guidelines specified by company policies or law-enforcement agencies

To exercise data protection we're committed to:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- Train employees in online privacy and security measures
- Build secure networks to protect online data from cyberattacks
- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses or communicate statements on how we handle data
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Together Software management will determine how serious an employee's offense is and take the appropriate action.

Further Questions and Responsibility

Any questions regarding the use of or suggested modifications to Non-Disclosure Agreements should be referred to the Security team.

It is the Security team's responsibility for ensuring this policy is followed.

Last updated: September 20, 2022

Disaster Recovery Plan

The Together Software Disaster Recovery Plan ("DRP") establishes procedures to recover Together Software operations following a disruption resulting from a disaster. The types of disasters contemplated by this plan include natural disasters, political disturbances, man made disasters, external human threats, and internal malicious activities. This DRP is maintained by the Security team.

Disaster Recovery Policies

- Together Software performs testing of the Disaster Recovery Plan annually. The Security team is responsible for coordinating and conducting rehearsals of this Disaster Recovery Plan annually.
- Whenever the DRP is used, it must be followed by a retrospective and tabletop reenactment in order to identify lessons learned and playbooks needing creation.
- This policy and plan must be updated at least annually with additional playbooks taking into account new risks of disasters learned through testing and reenactment of past disaster incidents.

Scope of Disaster Recovery Plan

This policy includes all resources and processes necessary for service and data recovery, and covers all information security aspects of business continuity management.

The following conditions must be met for this plan to be viable:

1. All equipment, software and data (or their backups/failovers) are available in some manner.
2. If an incident takes place at the organization's physical location, all resources involved in recovery efforts are able to be transferred to an alternate work site (such as their home office) to complete their duties.

This plan does not cover the following types of incidents:

1. Incidents that affect customers or partners but have no effect on Together Software's systems. In this case, the customer must employ their own continuity processes to make sure that they can continue to interact with Together Software systems.
2. Incidents that affect cloud infrastructure suppliers at the core infrastructure level, including but not limited to Google, Slack, and Amazon Web Services. The organization depends on such suppliers to employ their own continuity processes.

Notification List

In the event of a disaster, notify these people in order:

- Nathan Goldstein (Cofounder and Director of Security)
- Matthew Reeves (Cofounder and CEO)

Disaster Recovery Objectives

The objectives of this plan are the following:

- Identify the activities, resources, and procedures needed to carry out Together Software's processing requirements during prolonged interruptions to normal operations.
- Identify and define the impact of interruptions to Together Software's systems.
- Assign responsibilities to designated personnel and provide guidance for recovering Together Software operations during prolonged periods of interruption to normal operations.
- Ensure coordination with other Together Software staff who will participate in the contingency planning strategies.
- Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies. Please see Together Software's critical contacts on Together Software's Business Continuity Plan.

Defining Critical Systems and Services

From a disaster recovery perspective, Together Software defines two categories of systems:

Non-Critical Systems. These are all systems not considered critical by the definition below. 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. Non-Critical Systems are restored at a lower priority than Critical Systems. Examples of Non-Critical Systems include analytics servers.

Critical Systems. These systems host application servers and database servers or are required for the 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.

The following services and technologies are considered to be critical for Together Software business operations, and must immediately be restored (in priority order):

1. Production infrastructure
2. Transit infrastructure
3. Build and deployment infrastructure
4. 3rd Party Transactional Email Services

General Disaster Recovery Plan

While specific playbooks are available for specific scenarios, there are overall rules of engagement whenever a disaster incident needs to be opened.

Notification Phase

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to Together Software. The notification sequence is listed below:

1. The first person to report the disaster should notify Nathan Goldstein (Director of Security).
2. Nathan Goldstein (Director of Security) is to notify team members referenced above in the Notification List section.
3. Based on the damage assessment, if Together Software will be unavailable to customers for more than 24 hours, the Director of Security will declare that a disaster has occurred and that the Disaster Recovery Procedure has been activated. The Directory of Security also has the discretion to activate the Disaster Recovery Procedure based on other criteria.
4. In the event customer data has been compromised, customers must be notified no later

than 72 hours after the incident is reported.
5. Once the Disaster Recovery Procedure has been activated, the Director of Security should notify relevant personnel and executive leadership on the general status of the incident. Notification can be conducted over chat, email or phone. The Director of Security may also notify the Together Software operations team if the disaster involves the Together Software premises or is related to Together Software employees.
6. If the Disaster Recovery Procedure has not been activated, the Recovery and Reconstitution phases will not be performed. Instead, Director of Security and necessary team members will perform all appropriate tasks under Together Software's Incident Response Plan.
7. Either Director of Security or someone they select will document who was contacted and when and will summarize each call.

Recovery Phase

This phase covers the recovery of the application at an alternate site. If the disaster involves both Critical Systems and Non-Critical Systems, the Together Software Security Team may prioritize the recovery of Critical Systems and proceed to the Reconstitution Phase for the Critical Systems before Non-Critical Systems have completed the Recovery Phase. This phase consists of the following tasks, some of which can be run in parallel:

1. Assess damage to affected environments, prioritizing critical systems first. Document observations.
2. If possible, back up the affected environments in a forensically sound manner. Do not alter affected systems and applications in any manner.
3. Verify that previous backups of critical databases and systems recovery points are available before moving on to the Reconstitution Phase.

Reconstitution Phase

This phase consists of activities necessary for restoring Together Software operations to the original operating state (or permanently move operations to the new site or state, if necessary). If the disaster involves both Critical Systems and Non-Critical Systems, the Together Software Security team may prioritize reconstituting the Critical Systems before beginning reconstitution of the Non-Critical Systems. This phase consists of the following tasks, some of which can be run in parallel:

1. Begin replication of new environment using previously confirmed backups using automated and previously tested scripts.
2. Together Software utilizes multiple availability zones; however, if the primary region is unavailable replicated backups should be used to create a production environment in the failover region.
3. Test new environment using pre-written tests.
4. Test logging, security and alerting functionality.
5. Verify that systems are appropriately patched and up to date.
6. Deploy new environment to production.
7. Update DNS to new environment.

Forensics Phase

This phase consists of activities related to finding out the cause of the disaster, in cases where it is not immediately apparent. Upon the disaster incident being addressed, with customer data and Together Software operating infrastructure recovered and restored, it is appropriate to start the Forensics Phase. This phase consists of the following tasks, some of which can be run in parallel:

1. Ensure all logs from all systems, applications and databases involved in the incident have maintained their integrity in the centralized log repository.
2. If some logs did not reach the central log repository, ensure that missing system, database

and application logs are retrieved. Pay attention to time keeping and clock settings, so logs from different sources can be reconciled.
3. If applicable, transfer data to a log analyzer or test instance.
4. Target network, system, and user action logs for analysis. Analyse all logs manually or with tools, tests, and scripts that have already been previously tested.
5. Document all significant findings in the timeline.

Retrospective Phase

A retrospective of an event such as a disaster recovery incident allows for all parties to understand what happened in a clear and blame-free manner. A retrospective meeting should occur within 72 hours after such an incident has occurred.

1. All relevant parties and system owners should be identified and invited to a retrospective meeting.
2. A draft agenda and disaster timeline should be sent to everyone before the retrospective meeting.
3. Retrospectives are best facilitated with an unbiased third party who was not involved with working the incident. The facilitator should ask questions of meeting participants to illuminate the severity, impact, and any follow-ups.
4. Document the retrospective meeting.
5. Produce an incident report from the retrospective agenda, timeline, and meeting notes.

Reenactment / Test Phase

Unanticipated disasters are unlikely to have documented steps for resolution. Once an unanticipated incident concludes, it should be reenacted to analyze and document how to better respond in the future. If applicable:

1. Run a simulation of the event, as understood by the retrospective meeting notes, timeline, and report. The simulation can be run with people involved or uninvolved with the disaster.
2. While running the simulation, a pre-assigned note taker should write down ideas to prevent and mitigate a similar event.
3. After the reenactment, a new and specific disaster recovery procedure should be created.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Together Software management will determine how serious an employee's offense is and take the appropriate action.

Responsibility

The Security Team is responsible for ensuring this policy is followed.

Last updated: November

Incident Response Plan

This document offers guidance for employees or incident responders who believe they have discovered or are responding to a security incident.

Escalation

- Email security@togetherplatform.com or message #security or #general on Slack.
- Include as many specifics and details as you can.

Severity

Severity level	Description	Examples	Remediation
Low or Medium Severity	Most issues fall under this category. These do not require someone to be paged or woken up in the middle of the night.	Suspicious emails, outages, strange activity on a laptop	Sending a message to the #security or #general channel
High severity	These are problems where an adversary or active exploitation hasn't been proven yet, and an attack may not have happened, but is likely to happen.	Backdoors, malware, malicious access of business data (e.g. passwords, payment information, vulnerability data, etc.)	Sending a message to the #security or #general channel with an @channel notification to notify all participants, as well as an email to security@togetherplatform.com
Critical severity	The attackers were successful, and something was lost.		Sending a message to the #security or #general channel with an @channel notification to notify all participants, as well as an email to security@togetherplatform.com. Additionally, the CEO and CTO will be messaged via text-message until they have acknowledged receipt

Internal Issues

When the malicious actor is an employee, contractor, vendor, or partner, please contact the Security Team directly. Do not discuss the issue with other employees.

Compromised Communications

If there are IT communication risks (i.e. company phones, laptops, email accounts, etc. are compromised) the team will announce an out-of-band communication tool within the office.

Response Steps

For critical issues, the response team will follow an iterative response process designed to investigate, contain the exploitation, remediate the vulnerability, and write post mortem and lessons learned documents.

1. The Security Team should determine if a lawyer should be involved with attorney-client privilege
2. A "War Room" will be designated
3. The following meeting will take place at regular intervals, starting with twice per day, until the incident is resolved

Response Meeting - Agenda

- Customers and clients should be notified based on contractual requirements or without undue delay, whichever is sooner, upon becoming aware of an incident.
- Update the **Breach Timeline** with all known data related to the incident. The timeline should detail what you're sure the attacker did at what times.
- Review new **Indicators of Compromise** with the entire group. Indicators of Compromise are anything you know belongs to the attacker: an IP address that sent data, a compromised account, a malicious file used to spearphish, etc.
- Add new data (knowns and unknowns) to the **Investigative Q&A**, which is a list of questions to which, if you had answers, you'd understand everything the attacker did.
- Update the list of **Emergency Mitigations**: passwords to be reset, laptops to be wiped, IPs to be banned, etc.
- Long Term Mitigations (including Root Cause Analysis): record everything you'll start doing so this crisis doesn't happen again.
- Everything Else: communications, legal issues, blog posts, status pages, etc.
- Customers and clients should be notified of the incident response investigation results.

Response Team Members

- Nathan Goldstein (Nathan@togetherplatform.com)
- Vitalii Milanych (vitalii@togetherplatform.com)
- Matthew Reeves (matthew@togetherplatform.com)

Required Retrospective

All incidents classified as "High" or above require a retrospective meeting and a "lessons learned" document.

Follow-ups must be completed

All incidents classified as "Medium" or above require follow-ups to be tasked in a task tracker and completed within a pre-defined time period.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Together Software management will determine how serious an employee's offense is and take the appropriate action.

Responsibility

The Security Team is responsible for ensuring this policy is followed.

Last updated: January 10, 2024

Information Security Policy

Together Software is committed to conducting business in compliance with all applicable laws, regulations, and company policies. Together Software has adopted this policy to outline the security measures required to protect electronic information systems and related equipment from unauthorized use.

Overview

This Information Security Policy is intended to protect Together Software's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and file transfers, are the property of Together Software. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Together Software employee or contractor who deals with information and/or information systems. It is the responsibility of every team member to read and understand this policy, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to communicate our information security policies and outline the acceptable use and protection of Together Software's information and assets. These rules are in place to protect customers, employees, and Together Software. Inappropriate use exposes Together Software to risks including virus attacks, compromise of network systems and services, and legal and compliance issues.

The Together Software "Information Security Policy" is comprised of this policy and all Together Software policies referenced and/or linked within this document.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Together Software business or interact with internal networks and business systems, whether owned or leased by Together Software, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Together Software and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Together Software policies and standards, and local laws and regulations.

This policy applies to employees, contractors, consultants, temporaries, and other workers at

Together Software, including all personnel affiliated with third parties. This policy applies to all Together Software-controlled company and customer data as well as all equipment, systems, networks and software owned or leased by Together Software.

Leadership Roles and Responsibilities

This section and associated guidance establish the roles and responsibilities within Together Software, which is critical for effective communication of information security policies and standards. Roles are required within the organization to provide clearly defined responsibilities and an understanding of how the protection of information is to be accomplished. Their purpose is to clarify, coordinate activity, and actions necessary to disseminate security policy, standards, and implementation.

Roles	Responsibilities
Board of	Oversight over Cyber-Risk and internal control for information security, privacy and compliance

Directors	Consults with Executive Leadership to understand Together Software IT mission and risks and provides guidance to bring them into alignment
Executive Leadership	Approves Capital Expenditures for Information Security Oversight over the execution of the information security risk management program and risk treatments Communication Path to Together Software Board of Directors Aligns Information Security Policy and Posture based on Together Software's mission, strategic objectives and risk appetite

Information Security Roles and Responsibilities

Security Team	Oversight over the implementation of information security controls for infrastructure and IT processes Responsible for the design, development, implementation, operation, maintenance and monitoring of IT security controls Ensures IT puts into practice the Information Security Framework Responsible for conducting IT risk assessments, documenting the identified threats and maintaining risk register Communicates information security risks to executive leadership Reports information security risks annually to Together Software's leadership and gains approvals to bring risks to acceptable levels Coordinates the development and maintenance of information security policies and standards Works with applicable executive leadership to establish an information security framework and awareness program Serve as liaison to the Board of Directors, Law Enforcement, Internal Audit and General Council. Oversight over Identity Management and Access Control processes Oversight and implementation, operation and monitoring of information security tools and processes in customer environments Execution of customer data retention and deletion processes Manage the confidentiality, integrity and availability of the information systems for which they are responsible in compliance with Together Software policies on information security and privacy. Approval of technical access and change requests for non-standard access Responsible for oversight over third-party risk management process Oversight over information security in the software development process Responsible for the design, development, implementation, operation, maintenance and monitoring of development and commercial cloud hosting security controls Responsible for oversight over policy development Responsible for implementing risk management in the development process
Director of Security	Responsible for creating and enforcing security policies and procedures Leading the monitoring, vulnerability management, and incident detection and response initiatives Tracking and reducing risk organization-wide Ensuring appropriate testing and background checks are completed Ensuring that employees and relevant contractors are presented with company policies and the Code of Conduct (CoC) Ensuring that employee performance and adherence the CoC is periodically evaluated Ensuring that employees receive appropriate security training
Together Software	Acting at all times in a manner which does not place at risk the health and safety of themselves, other person in the workplace, and the information and resources they have use of

Employees, Contractors, temporary workers, etc.	Helping to identify areas where risk management practices should be adopted Taking all practical steps to minimize Together Software's exposure to contractual and regulatory liability Adhering to company policies and standards of conduct Reporting incidents and observed anomalies or weaknesses

Executive Leadership

The Together Executive Leadership team is comprised of the following staff: Matthew Reeves (CEO)

Security Team

The Together Software Security team is comprised of Together Software's following staff:

Nathan Goldstein

Vitalii Milanych

The team is responsible for carrying out all security policies and procedures. The team has a direct line to the CEO and can communicate with the CEO whenever they need to.

Director of Security

Nathan Goldstein is the Director of Security.

Security Incident Reporting

All users are required to report known or suspected security events or incidents, including policy violations and observed security weaknesses. Incidents should be reported immediately or as soon as possible by email to security@togetherplatform.com or message #security on Slack..

In your email please describe the incident or observation along with any relevant details.

Mobile Device Policy

All end-user devices (e.g., mobile phones, tablets, laptops, desktops) must comply with this policy. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

System level and user level passwords must comply with the Access Control Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

All end-user, personal (BYOD) or company owned devices used to access Together Software information systems (i.e. email) must adhere to the following rules and requirements:

Devices must be encrypted with a password-protected screensaver or screen lock after 5 minutes of non use

Devices must be locked whenever left unattended

Users must report any suspected misuse or theft of a mobile device immediately to the Together Security team

Confidential information must not be stored on mobile devices or USB drives (this does not apply to business contact information, e.g., names, phone numbers, and email addresses)

Any mobile device used to access company email must not be shared with any other person

Upon termination users agree to return all company owned devices and delete all company information and accounts from any personal devices

Remote Access Policy

Laptops and other computer resources that are used to access the Together Software network must conform to the security requirements outlined in Together Software's Information Security Policies and adhere to the following standards:

To ensure mobile devices do not connect a compromised device to the company network Users are prohibited from changing or disabling any organizational security controls on systems used to access Together Software resources

Use of remote access software and/or services (e.g., VPN client) is allowable as long as it is provided by the company and configured for multifactor authentication (MFA) Unauthorized remote access technologies may not be used or installed on any Together Software system

If you access from a public computer (e.g., business center, hotel, etc.), log out of session and don't save anything. Don't check "remember me, collect all printed materials and delete downloaded files (generally is discouraged)

Human Resource Policy

Screening

Background verification checks on Together Software personnel shall be carried out in accordance with relevant laws, regulations, and shall be proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. Background screening shall include criminal history checks unless prohibited by local statute. Together may rescind an employee's offer letter if their background check is found to be falsified, erroneous, or misleading.

Competence Assessment

The skills and competence of employees and contractors shall be assessed by human resources staff and the hiring manager or his or her designees as part of the hiring process. Required skills and competencies shall be listed in job descriptions and requisitions. Competency evaluations may include reference checks, education and certification verifications, technical testing, and interviews.

All Together Software employees will undergo a performance review on at least an annually basis which will include an assessment of job performance, competence in the role, adherence to company policies and code of conduct, and achievement of role-specific objectives.

Terms & Conditions of Employment

Company policies and information security roles and responsibilities shall be communicated to employees and third-parties at the time of hire or engagement. Employees and third-parties with access to company or customer information shall sign an appropriate non-disclosure or confidentiality agreement. Contractual agreements shall state responsibilities for information security as needed. Employees and relevant third-parties shall follow all Together Software information security policies.

Management Responsibilities

Management shall be responsible for ensuring that information security policies and procedures and reviewed annually, distributed and available, and that employees and contractors abide by those policies and procedures for the duration of their employment or engagement. Annual policy review shall include a review of any linked or referenced procedures, standards or guidelines.

Management shall ensure that information security responsibilities are communicated to individuals, through written job descriptions, policies or some other documented method which is accurately updated and maintained. Compliance with information security policies and procedures and fulfillment of information security responsibilities shall be evaluated as part of the performance review process wherever applicable.

Information Security Awareness, Education & Training

All Together Software employees and third-parties with administrative or privileged technical access to Together Software production systems and networks shall complete security awareness training at the time of hire. Management shall monitor training completion and shall take appropriate steps to ensure compliance with this policy. Employees and contractors shall be aware of relevant information security policies and procedures.

Together employees and contractors in developer roles are provided with SDLC / Secure Coding training during their first 30 days of employment and annually thereafter. Software developers are trained in secure coding techniques, including how to avoid common coding vulnerabilities. All such personnel are then required to acknowledge, electronically, that they have attended and understand SDLC training and OWASP Top Ten common coding vulnerabilities.

Termination Process

Employee and contractor termination and off boarding processes shall ensure that physical and logical access is promptly revoked in accordance with company SLAs and policies, and that all company issued equipment is returned or securely disposed of.

Any security or confidentiality agreements which remain valid after termination shall be communicated to the employee or contractor at time of termination.

Disciplinary Process

Employees and third-parties who violate Together Software information security policies shall be subject to the Together Software progressive disciplinary process, up to and including termination of employment or contract.

Additional Policies and Procedures Incorporated by Reference

Role	Purpose
Change Management Policy	To describe the rules for the acquisition and development of software and systems that shall be applied to developments within the Together Software organization
System Access Control Policy	To limit access to information and information processing systems, networks, and facilities to authorized parties in accordance with business objectives.
Asset Management Policy	To identify organizational assets and define appropriate protection responsibilities.
Business Continuity Plan & Disaster Recovery Plan	To prepare Together Software in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and torestore services to the widest extent possible in a minimum time frame.
Cryptography Policy	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
Data Classification Policy, Data Protection Policy, Data Deletion Policy	To ensure that information is classified and protected in accordance with its importance to the organization.
Incident Response Plan	Policy and procedures for suspected or confirmed information security incidents.
Physical Security Policy	To prevent unauthorized physical access or damage to the organization's information and information processing facilities.
Risk Management Policy	To define the process for assessing and managing Together Software's information security risks in order to achieve the company's business and information security objectives.

Password Policy

Together Software's Password Policy describes how employees should generate, store, and retrieve their passwords for cloud services they use on behalf of the company or personally.

Password Generation

Together Software employees must use complex passwords, where possible, for all of their accounts that have access to Together Software data.

A "Complex" password:

> Has a high level of randomness, called password entropy, which you can achieve using a long string of characters of different types, such as uppercase letters, lowercase letters, numerals, and special characters
>
> Is not a commonly used weak password, like "123456" or "password123"
>
> Is not easy to guess, such as simple words or phrases, or patterns in which the password is the same as the username
>
> Is not known to be compromised—that is, it's not in a database of breached accounts Is at least 10 characters long
>
> Cannot be reused within the last 10 previously used passwords.

All generated passwords for Together Software users and system accounts must be unique. Together Software employees may not reuse passwords that are or were used elsewhere, e.g. passwords used for personal accounts. A common way attackers obtain access to corporate resources is by using employees' personal passwords that were obtained in breaches of other services.

When creating end user passwords for the first time and/or during a password reset, the Security Team must also force the end user to change their password upon logging in for the first time.

Together Software employees must always use two-factor authentication for all accounts that have access to Customer-Confidential or Company-Confidential Together Software data.

Password Requirements from Services

The services that Together Software uses to provide its offering also enforce password rules, which all users (including Together Software employees) must follow.

Managing and Storing Passwords

Together Software employees are required to use password management software to manage their passwords and generate sufficiently complex passwords. The suggested password management software is specified in the Together onboarding document. If an Together employee wants to use another software, this must be approved by the security team first.

All Together Software system and user passwords must be encrypted when stored at rest within an application or database.

All Together Software system and user passwords must be encrypted during transmission.

Under no circumstances should Together Software employees share their account passwords with anyone, including other Together Software employees.

Single Sign-On Authorization

When available, single sign-on (SSO) should be considered the primary method of authorization for Together Software employees. This approach streamlines the authentication process and enhances security. Employees are encouraged to utilize SSO with vendors that support this feature.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Together Software management will determine how serious an employee's offense is and take the appropriate action:

> For minor violations, employees may only receive verbal reprimands.
>
> For more serious violations (e.g. a security incident or breach caused by reuse of personal passwords), employees may face severe disciplinary actions up to and including termination.

Responsibility

The Security team is responsible for ensuring this policy is followed.

Last updated: August 22, 2024

Physical Security Policy

Together Software's Physical Security Policy describes how staff should permit access to and secure the Together Software office.

Physical Office Access

Physical access to Together Software's office is controlled using a combination of key-cards, physical keys, and virtual access credentials. Only Together Software employees and building staff are authorized to possess these access tools.

- Together Software's office remains locked throughout the entire day.
- Together Software's office is an open space concept for collaborative reasons.
- Together Software reviews key, badge, and virtual access credentials to ensure all access methods are accounted for and only in the possession of current employees.
- Employees are required to immediately report lost or stolen badges, key-cards, or any issues with virtual access credentials to the building management.
- Upon the termination of employment, all forms of physical and logical access, including key-cards, physical keys, and virtual access credentials, are revoked. It is the responsibility of the Building Management to collect these items, along with company equipment and any other relevant property, from departing employees.

Security Surveillance

Together Software's office building has security cameras. Together Software has an agreement in place with building management to access camera footage in the event that it is needed.

Fire Alarms

Fire detectors are installed according to applicable laws and regulations.

Visitor Access Policy

Together Software employees may invite visitors to the office for business reasons or during pre-specified times, for social reasons. Together Software staff must escort and supervise their visitors at all times and are responsible for the visitors' behavior while they are in the office.

Visitors who misbehave (e.g. engage in hate speech, cause disruption, steal property, or take pictures of confidential data) will be asked to leave.

Visitor Sign-In Policy

Visitors are required to sign in. Visitors announce themselves to front desk staff, who have the visitor sign into building visitor system. Front desk staff have visitors wait in the lobby while the host is notified that their visitor has arrived. Hosts are required to collect their visitor and escort them throughout the visit.

Unauthorized Visitors

Together Software employees who spot unauthorized visitors should either ask the unauthorized person to leave or refer the issue to management.

Contractors and Service Vendors

Contractors, suppliers and service vendors, e.g. IT technicians, may enter Together Software's office to complete their job duties. The visitors' hosts are responsible for providing contractors and vendors with appropriate identification and direction while on Together Software's premises.

Deliveries

Anyone who delivers orders, mail, or packages for employees should remain at the building's reception or gate.

Large deliveries (e.g. supplies) should be delivered to designated spaces (e.g. store rooms).

Clean Desk Policy

To limit visitor exposure to sensitive information, Together Software implements a Clean Desk Policy, intended to be a set of behaviors all staff are to adhere to.

- All Together Software staff must wipe down whiteboards immediately after use.
- All Together Software staff must not leave sensitive written information on any desk surface.
- All Together Software staff must insert paper copies with sensitive data into secure paper destruction boxes.

Employee Identification and Access

For the physical security of Together Software's office space, virtual access credentials are now utilized. These credentials serve as both identification and access control, enabling staff to verify if individuals have authorization to be in the office space.

- Virtual access credentials are issued to all Together Software full-time employees and contractors who require office access. These credentials are provided on their first day of employment and are specifically programmed to identify them as either full-time employees or contractors.
- This policy applies only to employees and contractors who have office access. Not all employees are granted physical access to the office.
- Visitors are managed through a separate virtual visitor management system, which includes their name and a digital identifier. Visitors are required to have an escort at all times within the office premises.
- If an employee encounters an individual in the office space whose presence they are unaware of, or who appears to be without proper identification or an escort, they are required to report this immediately to office security or management. It's crucial for maintaining a secure and safe working environment.

Some Together Software employees are remote employees. Physical access to company laptops is secured in the same manner that someone would secure their own home.

Some employees are located in an outsourced office. Because office management is outsourced to One-Eleven, the physical security of the office is managed by One-Eleven for Together Software.

One-Eleven manage the following aspects of physical security for Together Software:

- Security alarms - Together Software office building has security alarms.
- Security surveillance - Together Software's office building has security cameras. Together Software has an agreement in place with building management to access camera footage in the event that it is needed.
- Fire alarms - Fire detectors are installed according to applicable laws and regulations.`

Securing Physical Laptops

All employees are required to secure their physical laptops in the following manner:

- The confidentiality, security and privacy of Together Software's customers must be preserved, by ensuring that no unauthorized individuals may view, overhear, or otherwise have access to Together Software's customer data.
- To enforce, all Together Software employees are provided with Privacy Screen Protectors for laptop monitors and are required to be aware of direct shoulder surfing when doing work in a public place such as a coffee shop or the airport. Together Software employees are further required not to teleconference with customers in public areas.
- All Together Software end user devices, such as laptops and cell phones containing access to internal Together Software resources, must be protected at all times and may not be left unattended.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Together Software management will determine how serious an employee's offense is and take the appropriate action:

- For minor violations (e.g. bringing in personal visitors without authorization), employees may only receive verbal reprimands.
- For more serious violations (e.g. bringing in unauthorized visitors who rob or damage company property), employees may face severe disciplinary actions up to and including termination.

Responsibility

The Security Team is responsible for ensuring this policy is followed.

Last updated: January 10, 2024

Responsible Disclosure Policy

Data security is a top priority for Together Software, and Together Software believes that working with skilled security researchers can identify weaknesses in any technology.

If you believe you've found a security vulnerability in Together Software's service, please notify us; we will work with you to resolve the issue promptly.

Disclosure Policy

- If you believe you've discovered a potential vulnerability, please let us know by emailing us at security@togetherplatform.com. We will acknowledge your email within five business days.
- Provide us with a reasonable amount of time to resolve the issue before disclosing it to the public or a third party. We aim to resolve critical issues within five business days of disclosure.
- Make a good faith effort to avoid violating privacy, destroying data, or interrupting or degrading the Together Software service. Please only interact with accounts you own or for which you have explicit permission from the account holder.

Exclusions

While researching, we'd like you to refrain from:

- Distributed Denial of Service (DDoS)
- Spamming
- Social engineering or phishing of Together Software employees or contractors
- Any attacks against Together Software's physical property or data centers

Thank you for helping to keep Together Software and our users safe!

Changes

We may revise these guidelines from time to time. The most current version of the guidelines will be available at https://help.togetherplatform.com/hc/en-us/articles/4401992412955-Security-Policies.

Contact

Together Software is always open to feedback, questions, and suggestions. If you would like to talk to us, please feel free to email us at security@togetherplatform.com.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Together Software management will determine how serious an employee's offense is

and take the appropriate action.

Responsibility

It is the Security team's responsibility to see this policy is enforced.

Last updated: September 22, 2022

Risk Assesment & Management Program

Purpose

To define principles and the methodology for assessing and managing Together Software's information security risks in order to achieve the company's business and information security objectives.

Scope

The risk assessment process may be applied to all business processes, information, information systems, networks, devices, and information processing facilities that are owned or used by Together Software applicants, employees, contractors, consultants, vendors, partners, and other users affiliated with Together Software, or others using or accessing Together Software networks and/or information systems.

Policy

Together Software will ensure that risk management plays an integral part in the governance and management of the organization at a strategic and operational level. The purpose of a risk management policy is designed to ensure that the company achieves its stated business and security goals and objectives.

Principles

Together is proactive in its approach to risk management, balances the cost of managing risk with anticipated benefits, and undertakes contingency planning in the event that critical risks are realized.

Together has the primary duty to ensure the Security, Availability, and Confidentiality of critical systems and customer data. A duty to ensure a secure, available infrastructure requires Together to identify and manage risks.

Together believes that effective risk management involves:

1. A commitment to the Security, Availability, and Confidentiality of Together infrastructure and services from senior management
2. The involvement, cooperation and insight of all Together staff
3. A commitment to initiating risk assessments, starting with discovery and identification of risks
4. A commitment to the thorough analysis of identified risks
5. A commitment to a strategy for treatment of identified risks
6. A commitment to communicate all identified risks to the company
7. A commitment to encourage the reporting of risks and threat vectors from all Together staff

Together believes that the following events can trigger a risk assessment to occur:

1. A significant and major change to existing infrastructure, product or business practices
2. A significant amount of time (e.g. a year) having passed since the last risk assessment

Risk assessments can be as high level or detailed to a specific organizational or technical change as Together stakeholders and technologists see fit.

Risk assessments can be conducted by unbiased and qualified parties such as security consultancies or qualified internal staff.

Risk Assessment Process

Together risk assessment methodology is based off NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments.

- Management defines the scope of risk assessment and creates the risk assessment team with a point person to guide the process (risk assessment project lead).
- If risk assessment procedures are not defined, the team should define them. The proper time and method of communicating the selected risk treatment options to the affected IT and business management should be included.
- Evaluate the system - Determine if the system is critical to the organization's business processes and determine the data classification and security needs of the data on the system according to the Together Data Classification Policy, considering Security, Availability, and Confidentiality needs.
- List the threats - List possible threat sources such as an exploitation of a vulnerability.
- Identify vulnerabilities.
- Evaluate potential security controls already in place to assess if they adequately address the risk.
- Identify probability of exploitation. Additional security controls may need to be in place before the probability of exploitation is lowered.
- Quantify damage (impact) - Categorize the damage and possibly place a dollar amount on the damage where possible. This will help when looking at cost of controls to reduce the risk.
- Determine risk level - Use likelihood times impact to quantify the amount of risk.
- Evaluate and recommend controls to reduce or eliminate risk - Identify existing controls and those that may further reduce probabilities or mitigate specific vulnerabilities. List specific threats and vulnerabilities for the system to help identify mitigating controls.
- Create the risk assessment report.
- Communicate the selected risk treatment options to the affected IT and business management and staff.
- Take recommended risk mitigation actions. Record such actions as changes per the Together Change Management program.
- Monitor the effectiveness of the risk mitigation actions and document the results.

Risk Management Strategy

Together Software has developed processes to identify those risks that would hinder the achievement of its strategic and operational objectives. Together Software will therefore ensure that it has in place the means to identify, analyze, control, and monitor the strategic and operational risks it faces using this risk management policy based on best practices.

The Director of Security will ensure the risk management strategy and policy are reviewed regularly and that:

- The risk management policy is applied to relevant areas at Together Software
- The risk management policy and its operational application are annually reviewed

- Non-compliance is reported to appropriate company officers and authorities

Practical Application of Risk Management

Together Software may use a variety of risk reporting formats for the identification of risks, their classification, and evaluation based on factors such as vendors utilized, methodology employed, and the scope of the assessment. In general, and where possible, risks shall be assessed and ranked according to their impact and their likelihood of occurrence. A formal IT risk assessment, network penetration tests, and Together Software production application penetration test will be performed at least annually.

In addition, an internal audit of the information security management system (ISMS) (i.e., information security controls and management processes) shall be performed at least annually.

Security risks shall be evaluated at various stages of the software design and development lifecycle as needed.

Risk Categories

Some risks are within the control of Together Software while others may be only to a lesser degree. Together Software will consider the risks within each of the following categories:

- Technical
- Reputational
- Contractual
- Economic/Financial
- Regulatory/Compliance
- Fraud

Each identified risk will be assessed as to its likelihood and impact. Likelihood can be assessed as not likely, somewhat likely, or very likely. Impact can be assessed as not impactful, somewhat impactful, and very impactful. The likelihood and impact will be considered together to formulate an overall risk ranking.

Risk Criteria

The criteria for determining risk is the combined likelihood and impact of an event adversely affecting the confidentiality, availability, integrity, or privacy of customer data, personally identifiable information (PII), or business critical systems.

For all risk inputs such as risk assessments, penetration tests, vulnerability scans, etc., Together Software management shall reserve the right to modify automated or third-party provided risk rankings based on its assessment of the nature and criticality of the system processing, as well as the nature, criticality and exploitability (or other relevant factors and considerations) of the identified vulnerability.

Risk Response and Treatment

Risks will be prioritized and mapped using the approach contained in this policy. The following responses to risk should be employed. Where Together Software chooses a risk response other than "Accept," it shall develop a Risk Treatment Plan.

- Mitigate: Together Software may take actions or employ strategies to reduce the risk.
- Accept: Together Software may decide to accept and monitor the risk at the present time. This may be necessary for some risks that arise from external events.
- Transfer: Together Software may decide to pass the risk on to another party. For example, contractual terms may be agreed to ensure that the risk is not borne by Together Software, or insurance may be appropriate for protection against financial loss.

- Avoid: The risk may be such that Together Software could decide to cease the activity or to change it in such a way as to end the risk.

Risk Management Procedure

The procedure for managing risk will meet the following criteria:

- Together Software will maintain a Risk Register and Treatment Plan.
- Risks shall be ranked by 'likelihood' and 'severity/impact' as critical, high, medium, low, or negligible.
- Overall risk shall be determined through a combination of likelihood and impact.
- Risks may be valuated to estimate potential monetary loss where practical, or may be considered relative to a control objective
- Together Software will respond to risks in a prioritized fashion. Remediation priority will consider the risk likelihood and impact, cost, work effort, and availability of resources. Multiple remediations may be undertaken simultaneously.
- Periodic reports will be made to the senior leadership of Together Software to ensure risks are being mitigated appropriately, and in accordance with business priorities and objectives.

Risk Acceptance Levels

Role	Responsibility
CEO	Ultimately responsible party for the acceptance and/or treatment of any risks to the organization.
Director of Security	Can approve the avoidance, remediation, transference, or acceptance of any risk cited in the Risk Register. This person shall be responsible for communicating risks to top management and the board and adopting risk treatments in accordance with executive direction.
Security team member	Shall be responsible for adherence to this policy.

Acceptable Risks

When the probability of threat materialization times maximum damage amount is less than $1000 annually, the risk is acceptable. For higher amounts, on a yearly basis, acceptance of the risk will depend on the cost of implementing measures to reduce the risk. If the risk cannot be reduced and the amount per year is greater than $50,000, the risk should be transferred by purchasing insurance.

Amendment & Termination of this Policy

Together Software reserves the right to modify, amend or terminate this policy at any time.

Exceptions

Requests for an exception to this Policy must be submitted to the Together Software Security team for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the Together Software Security team. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Last updated: December , 2022

Appendix A: Risk Assessment Matrix and Description Key

	RISK = LIKELIHOOD * IMPACT	LIKELIHOOD		
		Very likely: 3	Somewhat likely: 2	Not likely: 1
IMPACT	Very impactful: 3	9	6	3
	Somewhat impactful: 2	6	4	2
	Not impactful: 1	3	2	1

RISK LEVEL	RISK DESCRIPTION
Low (1-2)	A threat event could be expected to have a limited adverse effect on organizational operations, mission capabilities, assets, individuals, customers or other organizations.
Moderate (3-6)	A threat event could be expected to have a serious adverse effect on organizational operations, mission capabilities, assets, individuals, customers or other organizations
High (7-9)	A threat event could be expected to have a severe adverse effect on organizational operations, mission capabilities, assets, individuals, customers or other organizations.

IMPACT LEVEL	IMPACT DESCRIPTION
Not impactful (1)	A threat event could be expected to have a limited adverse effect, meaning: degradation of mission capability yet primary functions can still be performed; minor damage; minor financial loss; or range of effects is limited to some cyber resources but no critical resources.
Somewhat impactful (2)	A threat event could be expected to have a serious adverse effect, meaning: significant degradation of mission capability yet primary functions can still be performed at a reduced capacity; minor damage; minor financial loss; or range of effects is significant to some cyber resources and some critical resources.
Very impactful (3)	A threat event could be expected to have a severe or catastrophic adverse effect, meaning: severe degradation or loss of mission capability and one or more primary functions cannot be performed; major damage; major financial loss; or range of effects is extensive to most cyber resources and most critical resources.

LIKELIHOOD LEVEL	LIKELIHOOD DESCRIPTION
Not likely (1)	Adversary is unlikely to initiate a threat event; non-adversarial threat event (e.g., nature, error, accident) is unlikely to occur; or threat is unlikely to have adverse impacts.
Somewhat likely (2)	Adversary is somewhat unlikely to initiate a threat event; non-adversarial threat event (e.g., nature, error, accident) is somewhat unlikely to occur; or threat is somewhat unlikely to have adverse impacts.
Very likely (3)	Adversary is highly likely to initiate a threat event; non-adversarial threat event (e.g., nature, error, accident) is highly likely to occur; or threat is highly likely to have adverse impacts.

System Access & Authorization Control Policy

Each Together Software employee, contractor, and associate has limited access to Together Software systems and applications. Access is always provisioned on a minimum-necessary (least-privilege) basis.

Employee Access to Together Software Systems

Access to Together Software systems and third-party accounts owned by Together Software will only be granted on a need-to-use basis, as defined by the responsibilities of the position held and the duties of that position.

Access control and management is divided into multiple phases of an account lifecycle: creation, privilege management, authorization, password management, audit, and revocation.

Authorization: Role Based Access Control

- In most cases, Together Software employees are granted access to Together Software systems according to their role and/or team.
- The executive team and team managers are jointly responsible for maintaining a list of roles and associated access scope for team members.
- If a Together Software employee requires access outside of the standard for their role or team, either they or their managers may initiate an access request, following the policy outlined in "access requests" below.

Creation: Access Requests

- Access requests for Together Software employees are made by employees and their managers.
- Access requests should be made to the Together Software employee or employees who manage the relevant resource(s).
- Those employees will not grant access unless they are satisfied the additional access is necessary for the grantee to complete a necessary business task.
- When granting access, employees will ensure grants are scoped to the minimum breadth and duration to complete the relevant business task. Root access will not be granted unless absolutely necessary to perform the job function.
- In addition, the employee(s) must accept the company's Acceptable Use Policy before access will be granted.

Privilege Management

- Together Software's Security team will determine and maintain appropriate assignment of privilege within Together Software's production, development and test applications and environments.
- Together Software's Security team will determine and maintain appropriate assignment of privilege within Together Software's databases.

- Together Software's Security team will determine and maintain appropriate assignment within supporting infrastructure.

Account Audit

- The responsible team will conduct quarterly audits of accounts, privileges and password management, and is required to document findings and changes in Jira.

Revocation: Role Changes & Termination

- Managers must notify Together Software's Security Team if an employee has been terminated or changes role.
- In the case of termination, the former employee's access is required to be revoked within reasonable timelines as defined by company procedural commitments in Vanta.
- In the case of a role change, the employee's access should be revised within reasonable timelines as defined by company procedural commitments in Vanta.
- In some cases, access will be revoked as a disciplinary measure for policy violation.

Employee Authentication to Together Software Systems

Authentication

Each Together Software employee has a unique user ID and password that identifies them as the user of a Together Software IT asset or application. All assets, applications and vetted third party platforms may be required to have two-factor authentication configured.

Password, Key, and Certificate Management

As specified in the Acceptable Use Policy and Password Policy, Together Software employees must use complex passwords and multi-factor authentication for all Together Software-related accounts. User passwords must conform with the restrictions set forward in the Together Software Password Policy. Please see Acceptable Use Policy and Password Policy for further details and guidance.

Together Software's Security Team is responsible for issuing and revoking SSH keys in all environments.

Together Software's Security Team is responsible for issuing, renewing, and revoking public web and internal SSL certificates.

Customer Data

Employees that require access to customer data must have an individual account. This account, as well as actions performed with it, will be subject to additional monitoring at the discretion of the management team and subject to applicable regulations and third-party agreements.

At a minimum, employees with access to customer data can expect that their actions in customer-data systems (e.g. an internal admin tool) will be logged, with the logs stored centrally for at least 12 months.

Guest Access to Together Software Systems

Occasionally, guests will have a legitimate business need for access to the corporate network. When such need is demonstrated, temporary guest access to company systems is permitted. This access, however, must be severely restricted to only those resources that the guest needs at that time, and disabled when the guest's work is completed.

Guest Wireless Use

Together Software's production systems are not accessible directly over wireless channels and connecting to the company guest wireless network should grant no extra privileges or access to company systems.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Together Software management will determine how serious an employee's offense is and take the appropriate action:

- For minor violations, employees may only receive verbal reprimands.
- For more serious violations that lead to security incidents, employees may face severe disciplinary actions up to and including termination.
- Together Software employees will not be disciplined for surfacing deficiencies or misconfigurations that contradict this policy.

Responsibility

Each Together Software employee is responsible for surfacing technical misconfigurations and deficiencies to the Security team for immediate resolution.

The Security Team is responsible for ensuring this policy is followed.

Last updated: September 22, 2022

Vendor Management Policy

Together Software relies on vendors to perform a range of services, some of which are critical for operations.

Together Software aims to manage its relationship with vendors and minimize the risk associated with engaging third parties to perform services. This policy provides a framework for managing the lifecycle of vendor relationships.

Vendor Risk Assessment

For each potential vendor, conduct an initial risk analysis, assigning the vendor a "low," "medium," or "high" rating based on the highest risk level attributable to the contract.

	Low	**Medium**	**High**
Business impact	Nominal impact, could get along without it. Does not connect to any piece of Together Software infrastructure.	Significant but non-critical business impact	Mission critical
Customer facing?	No	Indirect	Direct
Access to customer data	No access	Access to often public but personally-identifiable information (e.g. email addresses)	Access to non-public personally-identifiable information (e.g. email content)

The rating indicates the level of due diligence Together Software requires for each vendor:

- **Low-risk** vendors typically require little analysis
- **Medium-risk** vendors should be evaluated to determine the appropriate level of due diligence required
- **High-risk** vendors require extensive review

Vendor Assessment Process

Risk assessments should be conducted before doing business with a new vendor and revisited when the relationship with the vendor changes significantly, including contract renewals. All vendors are required to be reassessed annually.

An assessment of the proposed vendor is initiated when a Vendor Sponsor (anyone at Together Software looking to do business with a vendor) submits a review request to the Security Team.

The Vendor Sponsor may wish to sign a mutual Non-Disclosure Agreement (mNDA) with the proposed vendor. The proposed vendor and the Vendor Sponsor should sign the mNDA before the Vendor Sponsor:

- discloses Together Software information to determine company/vendor fit

- accepts a completed Vendor Assessment Questionnaire (VAQ), which contains the vendor's operating information.

The Vendor Sponsor should then submit the mNDA (if applicable), VAQ, and other relevant collateral to the Security Team for review.

The Security Team will complete the review in a timely manner and communicate next steps to the Vendor Sponsor. All reviews should be documented in meeting notes, for security, legal, and audit.

When the Security team approves the vendor, the Together Software Vendor Sponsor may move forward with contract negotiations.

The Security team must provide documented approvals to the Vendor Sponsor.

The Vendor Sponsor may set the vendor up for payment. The Vendor Sponsor will be responsible for ensuring the Security team documented their signoff.

Vendor Assessment Due Diligence

Due diligence entails making a reasonable inquiry into a vendor's ability to meet the requirements for the proposed service.

The Security Team will first perform primary research on the vendor, such as that of reputation and customer referrals / recommendations. Based on that, the Security Team may elect to send the proposed vendor a Vendor Assessment Questionnaire, or jump on a call with technical representatives from the Vendor. Once the VAQ/call is completed, a due diligence review includes further consideration of the following topics:

- **Regulatory**: Can the vendor create regulatory risk for Together Software?
- **Reputation**: How might the vendor impact Together Software's reputation?
- **Financial**: Can the vendor impact Together Software or its customers financially?
- **Access to customer data**: To what extent will the vendor handle sensitive Together Software data?
- **Operational effectiveness**: How might Together Software be affected if the vendor experienced downtime? If the vendor ceased operations suddenly? Are there other potential vendors that Together Software could work with in such cases?
- **Compensating controls:** Does the vendor offer multi-factor authentication on its service? Can that be enforced such that all Together Software users must turn on MFA to use the service?

Once the Security Team reviews the VAQ/Call responses and the above considerations, they will either clear the vendor, reject the vendor, or request further information.

Vendor Compliance Considerations

If the vendor has a SOC 2, ISO27001/2, or other relevant collateral, and is deemed a "high" risk vendor, it should be collected, reviewed by the Security team, and documented in Together Software records.

Managing Vendors

Vendor Supervision

Each vendor will be assigned a Vendor Sponsor who will act as a liaison between the vendor and Together Software.

Vendor List

The Security team maintains a complete list of all vendors, associated risk rankings, the Vendor Relationship Manager, and the date of the most recent evaluation.

Vendor Configuration

Multi-factor authentication should be enabled on all accounts for all vendors.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Together Software management will determine how serious an employee's offense is and take the appropriate action:

- For minor violations, employees may only receive verbal reprimands.
- For more serious violations (e.g. onboarding a vendor without appropriate review and due diligence), employees may face severe disciplinary actions up to and including termination.

Responsibility

The Together Software Vendor Sponsor is responsible for ensuring prospective vendors enter the vendor review process.

The Security team is responsible for ensuring this policy is followed.

Last updated: September 2, 2022

Vulnerability Management & Patch Program

Together Software's Vulnerability Management policies and procedures describe what systems are in place to monitor for new vulnerabilities, how often vulnerabilities are addressed, and the way in which those vulnerabilities are addressed.

On average, 20-30 new vulnerabilities are released into the wild every day. Together Software's internal vulnerability monitoring and external vulnerability scanning are in place to keep up with new threats while validating security controls put in place so that Together Software's security posture is maintained.

Vulnerability Management & Patch Policy

Systems and networks shall be provisioned and maintained in accordance with the configuration and hardening standards in section Severity & Timing of this policy.

Logging & Monitoring

Production infrastructure shall be configured to produce detailed logs appropriate to the function served by the system or device. Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and reviewed through manual or automated processes as needed. Appropriate alerts shall be configured for events that represent a significant threat to the confidentiality, availability or integrity of production systems or Confidential data.

Together Software performs internal vulnerability scanning and package monitoring on a constant basis using:

- Google Cloud Platform
  - Security Command Center
  - Container Analysis + Scanning API
  - GitHub
  - Vanta
  - Sentry

The Security team is responsible for communicating detected vulnerabilities and package updates needed to the appropriate engineering staff for resolution. Engineering staff responsible for various infrastructure components are responsible for resolving detected vulnerabilities in a timely manner as defined by Together Software's timing standards, as defined below.

Protection of Log Information

Logging facilities and log information shall be protected against tampering and unauthorized access.

Administrator & Operator Logs

System administrator and system operator activities shall be logged and reviewed and/or alerted in accordance with the system classification and criticality.

Clock Synchronization

The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to network time servers using reputable time sources.

Severity & Timing

Together Software defines the severity of an issue the score surfaced by the vulnerability scanning tool in use. If the vulnerability scanning tool does not provide a score, the Common Vulnerability Scoring System (CVSS) score is used. These scores capture the characteristics of a vulnerability and are translated into a qualitative representation (such as low, medium, high) to help organizations properly assess and prioritize their vulnerability management processes.

All vulnerabilities will be addressed within timelines defined below by severity:

- Low Severity: 90 days
- Medium Severity: 60 days
- High Severity: 30 days
- Critical Severity: 14 days

Low Severity - 0.1 - 3.9

Low severity vulnerabilities are likely to have very little impact on the business, perhaps because they require local system access.

Medium Severity - 4.0 - 6.9

Medium severity vulnerabilities usually require the same local network or user privileges to be exploited.

High Severity - 7.0 - 8.9

High severity vulnerabilities could result in escalated privileges, significant data loss, and/or downtime. They could lead to root level compromise of servers, applications, and other infrastructure components. If a high severity vulnerability cannot be addressed within timelines as defined, an incident response ticket will be opened, documenting what interim remediation has been made.

Critical - 9.0 - 10.0

If a critical severity vulnerability cannot be addressed within timelines as defined, an incident response ticket will be opened, documenting what interim remediation has been made.

Vulnerability & Patch Management Process

1. A new vulnerability or a new patch is detected from the various monitoring and scanning Together Software has in place, such as Vanta.
2. The Security Team enters vulnerability details or patch instructions into Together Software's change management system, which is Jira, and assigns the ticket to the appropriate team member to address.
3. The ticket assignee follows the change management process to implement the necessary change to apply the patch or address the new vulnerability.
4. The ticket is updated with results from the applied change, detailing any exceptions into

the Together Software risk register.
5. The Security Team checks the source from which the vulnerability originated to ensure that the change performed has addressed the vulnerability detected. The ticket is updated with the results, and closed out.

Exceptions

Any exception to the policy must be approved by the Security Team in advance and placed on the risk register for monitoring and periodic review.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including employment termination.

Responsibility

It is the Security Team's responsibility to ensure this policy is followed.

Reviewing vulnerability scans and continuous monitoring findings, and dividing up resolution tasks, are the responsibility of the Security Team.

All engineers and developers are responsible for investigating and resolving vulnerabilities assigned to them via patching and configuration changes, as they are assigned.

Last updated: Dec 5, 2022