LOGO PLACEHOLDER

Security Policy Packet

Security policies, code of conduct, and business continuity policies and procedures

[COMPANY] - RESTRICTED DATA

Table of Contents

Access Control Policy

Policy Owner: [NAME]

Effective Date: [DATE]

Purpose: To limit access to information and information processing systems, networks, and facilities.

Scope: All [Company] information systems that process, store, or transmit confidential data as defined in the [Company] Data Management Policy. This policy applies to all employees of [Company] and to all external parties with access to [Company] networks and system resources.

Policy: [Company] shall determine the type and level of access granted to individual users based on the "principle of least privilege." This principle states that users are only granted the level of access absolutely required to perform their job functions, and is dictated by [Company]'s business and security requirements. [Company]'s primary method of assigning and maintaining consistent access controls and access rights shall be through the implementation of Role-Based Access Control (RBAC).

Wherever feasible, rights and restrictions shall be allocated to groups. Individual user accounts may be granted additional permissions as needed with approval from the system owner or authorized party.

All privileged access to production infrastructure shall use Multi-Factor Authentication (MFA).

Access to information computing resources is limited to personnel with a business requirement for such access. Access rights shall be granted or revoked in accordance with this Access Control Policy.

Access to Networks and Services

The following security standards shall govern access to [Company] networks and network services:

- Only authorized [Company] employees and third-parties working off a signed contract or statement of work, with a business need, shall be granted access to the [Company] production networks and resources.
- [Company] guests may be granted access to guest networks after registering with office staff without a documented request.
- Remote connections to production systems and networks must be encrypted

User Access Management

[Company] requires that all personnel have a unique user identifier for system access, and that user credentials and passwords are not shared between multiple personnel. Users with multiple levels of access (e.g. administrators) should be given separate accounts for normal system use and for administrative functions wherever feasible. Root, service, and administrator accounts may use a password management system to share passwords for business continuity purposes only. Administrators shall only use shared administrative accounts as needed. If a password is compromised or suspected of compromise the incident should be escalated to the [designated employee overseeing IT] or responsible party to delegate to incident response immediately and the password must be changed.

User Registration and Deregistration

Only authorized administrators shall be permitted to create new user IDs, and may only do so upon receipt of a request from authorized parties. User provisioning requests must include approval from data owners or [Company] management authorized to grant system access. Prior to account creation, administrators should verify that the account does not violate any [Company] security or system access control policies such as segregation of duties, fraud prevention measures, or access rights restrictions. User IDs shall be promptly disabled or removed when users leave the organization or contract work ends in accordance with SLAs. User IDs shall not be re-used.

User Access Provisioning

New employees and/or contractors are not to be granted access to any [Company] production systems until after they have completed all HR on-boarding tasks, which may include but is not limited to signed employment agreement, intellectual property agreement, and acknowledgement of [Company]'s information security policy. Access should be restricted to only what is necessary to perform job duties, and no access may be

granted earlier than the official employee start date. No permissions shall be granted without approval from the system or data owner or management.

Management of Privileged Access

Granting of administrative rights shall be strictly controlled, and requires approval from the asset owner.

Removal and Adjustment of Access Rights

The access rights of all users shall be promptly removed upon termination of their employment or contract, or when rights are no longer needed due to a change in job function or role. The maximum allowable time period for access termination is 3 business days.

Segregation of Duties

Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of [Company] assets. When provisioning access, care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered when determining access levels for individuals and groups.

User Responsibilities

Control and management of individual user passwords is the responsibility of all [Company] personnel and third-party users. Users shall protect secret authentication information in accordance with the Information Security Policy.

Password Policies

Where feasible, passwords for confidential systems shall be configured consistent with the following requirements:

- A minimum of 16 characters, with alphanumeric and special characters
- Initial passwords must be set to a unique value and changed after first log in
- For manual password resets, a user's identity must be verified prior to changing passwords
- Do not limit the permitted characters that can be used

- Do not limit the length of the password to anything below 64 characters
- Do not use secret questions (place of birth, etc) as a sole password reset requirement
- Require the current password in addition to the new password during password change
- Verify newly created passwords against common passwords lists or leaked passwords databases
- Store passwords in a hashed and salted format using a memory-hard or CPU-hard one-way hash function
- Enforce appropriate account lockout and brute-force protection on account access

Password Management System

Systems for managing passwords should be interactive and assist [Company] personnel in maintaining password standards by enforcing password strength criteria including minimum length, and password complexity where feasible. All storage and transmission of passwords is to be protected using appropriate cryptographic protections, either through hashing or encryption.

System and Application Access Information Access Restriction

Applications must restrict access to program functions and information to authorized users and support personnel in accordance with the defined access control policy. The level and type of restrictions applied by each application should be based on the individual application requirements, as identified by the data owner. The application-specific access control policy must also conform to [Company] policies regarding access controls and data management.

Prior to implementation, evaluation criteria are to be applied to application software to determine the necessary access controls and data policies. Assessment criteria include, but are not limited to:

- Sensitivity and classification of data.
- Risk to the organization of unauthorized access or disclosure of data
- The ability to, and granularity of, control(s) on user access rights to the application and data stored within the application
- Restrictions on data outputs, including filtering sensitive information, controlling output, and restricting information access to authorized personnel

- Controls over access rights between the evaluated application and other applications and systems
- Programmatic restrictions on user access to application functions and privileged instructions
- Logging and auditing functionality for system functions and information access
- Data retention and aging features

All unnecessary default accounts must be removed or disabled before making a system available on the network. Specifically, vendor default passwords and credentials must be changed on all [Company] systems, devices, and infrastructure prior to deployment. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, and Simple Network Management Protocol (SNMP) community strings where feasible.

Access to Program Source Code

Access to program source code and associated items, including designs, specifications, verification plans, and validation plans shall be strictly controlled in order to prevent the introduction of unauthorized functionality into software, avoid unintentional changes, and protect [Company]'s intellectual property. All access to source code shall be based on business need and must be logged for review and audit.

Exceptions

Requests for an exception to this Policy must be submitted to the IT Manager for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the IT Manager. 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.

Asset Management Policy

Policy Owner: [Name]

Effective Date: [Date]

Purpose: To identify organizational assets and define appropriate protection responsibilities. To ensure that information receives an appropriate level of protection in accordance with its importance to the organization. To prevent unauthorized disclosure, modification, removal, or destruction of information stored on media.

Scope: This policy applies to all [Company] owned or managed information systems.

Policy: Assets will be managed in accordance with the outlined asset management policy.

Inventory of Assets

Assets associated with information and information processing facilities that store, process, or transmit confidential information shall be identified and an inventory of these assets shall be created and maintained.

Ownership of Assets

Assets maintained in the inventory shall be owned by a specific individual or group within [Company].

Acceptable Use of Assets

Rules for the acceptable use of information, assets, and information processing facilities shall be identified and documented in the Information Security Policy.

Loss of Theft of Assets

All [Company] personnel must immediately report the loss of any information systems, including portable or laptop computers, smartphones, PDAs, authentication tokens (keyfobs, one-time-password generators, or personally owned smartphones or devices with a [Company] software authentication token installed) or other devices that can store and process or help grant access to [Company] data.

Return of Assets

All employees and third-party users of [Company] equipment shall return all of the organizational assets within their possession upon termination of their employment, contract, or agreement.

Handling of Assets

Employees and users who are issued or handle [Company] equipment are expected to use reasonable judgment and exercise due care in protecting and maintaining the equipment. Employees are responsible for ensuring that company equipment is secured and properly attended to whenever it is transported or stored outside of company facilities.

All mobile devices shall be handled in accordance with the Information Security Policy. Except for employee-issued devices, no company computer equipment or devices may be moved or taken off-site without appropriate authorization from management.

Asset Disposal and Reuse

Company devices and media that stored or processed confidential data shall be securely disposed of when no longer needed. Data must be erased prior to disposal or re-use, using an approved technology in order to ensure that data is not recoverable. Or a Certificate of Destruction (COD) must be obtained for devices destroyed by a third-party service.

Customer Asset Return

Any physical assets owned by customers shall be promptly returned to the customer following service termination in accordance with the terms of contract or service agreement.

Exceptions

Requests for an exception to this policy must be submitted to the CEO or [designated employee overseeing IT] for approval.

Violations and Enforcement

Any known violations of this policy should be reported to the CEO and [designated IT lead] . Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance

Code of Conduct

Policy Owner: [Name]

Effective Date: [Date]

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

This code of conduct outlines our expectations for all [Company] staff, as well as the consequences for unacceptable behavior.

Scope: The Code of Conduct applies to all [Company] 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 [Company] office, during [Company]-related extracurricular activities and events, while attending conferences and other professional events on behalf of [Company], and while working remotely and communicating on [Company] resources with other staff.

We expect all [Company] 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 [Company] 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 [Company] staff and clients.

Policy: The policy is as outlined below.

Culture and 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 [Company] culture.

Be considerate. Your work at [Company] 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 nor pleasant.

[Company] should always be respectful when dealing with other personnel as well as with people outside of [Company] employment.

Acceptable and Expected Behavior

The following behaviors are expected and requested of all [Company] staff:

- Participate in an authentic and active way. In doing so, you contribute to the health and longevity of [Company]
- 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 [Company] leaders if you notice a dangerous situation, someone in distress, or violations of this Code of Conduct, even if they seem inconsequential.

Remember that [Company] events may be shared with members of the public and [Company] 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 [Company] 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. [Company] staff are further expected to comply with all state and local laws on this matter.

Consequences of Unacceptable Behavior

Unacceptable behavior from any [Company] 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, [Company] 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 [Company] 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. [Company] 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.

Cryptography Policy

Policy Owner: [Name]

Effective Date: [Date]

Purpose: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information. This policy establishes requirements for the use and protection of cryptographic keys and cryptographic methods throughout the entire encryption lifecycle.

Scope: All information systems developed and/or controlled by [Company] which store or transmit confidential data as defined in the Data Management Policy.

Policy: [Company] shall evaluate the risks inherent in processing and storing data, and shall implement cryptographic controls to mitigate those risks where deemed appropriate.

Where encryption is in use, strong cryptography with associated key management processes and procedures shall be implemented and documented.

Customer or confidential company data must utilize strong ciphers and configurations in accordance with vendor recommendations and industry best practices including NIST when stored or transferred over a public network.

Key Management

Access to keys and secrets shall be tightly controlled in accordance with the Access Control Policy.

The following table includes the recommended usage for cryptographic keys:

Domain	Key Type	Algorithm	Key Length	Max Expiration
Web Certificate	RSA or ECC with SHA2+ signature	RSA or ECC with SHA2+ signature	2048 bit or greater/RSA, 256 bit or greater/ECC	Up to 1 year
Web Cipher (TLS)	Asymmetric Encryption	Ciphers of B or greater grade on SSL Labs Rating	Varies	N/A
Confidential Data at Rest	Symmetric Encryption	AES	256 bit	1 Year

Exceptions

Requests for an exception to this policy must be submitted to the CEO or [designated security or engineering employee] for approval.

Violations and Enforcement

Any known violations of this policy should be reported to the CEO and [designated security or engineering employee]. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance

Data Management Policy

Policy Owner: [Name]

Effective Date: [Date]

Purpose: To ensure that information is classified, protected, retained and securely disposed of in accordance with its importance to the organization.

Scope: All [Company] data, information and information systems.

Policy: [Company] classifies data and information systems in accordance with legal requirements, sensitivity, and business criticality in order to ensure that information is given the appropriate level of protection. Data owners are responsible for identifying any additional requirements for specific data or exceptions to standard handling requirements. Information systems and applications shall be classified according to the highest classification of data that they store or process.

Data Classification

Confidential

Highly sensitive data requires the highest levels of protection; access is restricted to specific employees or departments, and these records can only be passed to others with approval from the data owner, or a company executive. Example include:

- Customer Data
- Company financial and banking data
- Salary, compensation and payroll information
- Strategic plans
- Incident reports
- Risk assessment reports

Confidential data should be labeled "confidential" whenever paper copies are produced for distribution.

Public

Documents intended for public consumption which can be freely distributed outside [Company]. Examples include:

- Marketing materials
- Product descriptions
- Release notes
- External facing policies

Data Handling

Confidential Data Handling

Confidential data is subject to the following protection and handling requirements:

- Access for non-pre approved roles requires documented approval from the data owner
- Access is restricted to specific employees, roles and/or departments
- Confidential systems shall not allow unauthenticated or anonymous access
- Confidential Customer Data shall not be used or stored in non-production engineering systems/environments
- Confidential Data will not be stored on personally owned devices of [Company] employees or contractors
- Confidential data shall be encrypted at rest and in transit over public networks in accordance with the Cryptography Policy
- Mobile device hard drives containing confidential data, including laptops, shall be encrypted
- Mobile devices storing or accessing confidential data shall be protected by a log-on password (or equivalent, such as biometric) or passcode and shall be configured to lock the screen after five (15) minutes of non-use
- Backups shall be encrypted
- Confidential data shall not be stored on personal phones or devices or removable media including USB drives, CD's, or DVD's
- Paper records shall be labeled "confidential" and securely stored and disposed of in a secure, approved manner in accordance with data handling and destruction policies and procedures
- Hard copy paper records shall only be created based on a business need and shall be avoided whenever possible

- Hard drives and mobile devices used to store confidential information must be securely wiped prior to disposal or physically destroyed
- Transfer of confidential data to people or entities outside the company shall only be done in accordance with a legal contract or arrangement, and the explicit written permission of management or the data owner

Public Data Handling

No special protection or handling controls are required for public data. Public data may be freely distributed.

Data & Device Disposal

Data classified as restricted or confidential shall be securely deleted when no longer needed. [Company] shall assess the data and disposal practices of third-party vendors in accordance with the Third-Party Management Policy. Only third-parties who meet [Company] requirements for secure data disposal shall be used for storage and processing of restricted or confidential data. [Company] shall ensure that all restricted and confidential data is securely deleted from company devices prior to, or at the time of, disposal.

Confidential and Restricted hardcopy materials shall be shredded or otherwise disposed of using a secure method. Personally identifiable information (PII) shall be collected, used and retained only for as long as the company has a legitimate business purpose. PII shall be securely deleted and disposed of following contract termination in accordance with company policy, contractual commitments and all relevant laws and regulations. PII shall also be deleted in response to a verified request from a consumer or data subject, where the company does not have a legitimate business interest or other legal obligation to retain the data.

Annual Data Review

Management shall review data retention requirements during the annual review of this policy. Data shall be disposed of in accordance with this policy.

Legal Requirements

Under certain circumstances, [Company] may become subject to legal proceedings requiring retention of data associated with legal holds, lawsuits, or other matters as

stipulated by [Company] legal counsel. Such records and information are exempt from any other requirements specified within this Data Management Policy and are to be retained in accordance with requirements identified by the Legal department. All such holds and special retention requirements are subject to annual review with [Company]'s legal counsel to evaluate continuing requirements and scope.

Policy Compliance

[Company] will measure and verify compliance to this policy through various methods, including but not limited to, technical controls and internal audits.

Exceptions

Requests for an exception to this policy must be submitted to the CEO or [designated security or IT employee] for approval.

Violations and Enforcement

Any known violations of this policy should be reported to the CEO and [designated security or IT employee] . Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance

Human Resource Security Policy

Policy Owner: [Name]

Effective Date: [Date]

Purpose: To ensure that employees and contractors meet security requirements, understand their responsibilities, and are suitable for their roles.

Scope: This policy applies to all employees of [Company], consultants, contractors and other third-party entities with access to [Company] production networks and system resources.

Policy: The human resource security policy is as outlined below.

Competence & Performance 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, and/or aligned with the responsibilities outlined in the Roles and Responsibilities Policy.

Competency evaluations may include reference checks, education and certification verifications, technical testing, take-home projects, and interviews.

All [Company] employees will undergo an annual performance review 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, and employees and contractors are required to formally acknowledge their understanding and acceptance of their security responsibilities. Employees and third-parties with access to company or customer information shall sign an appropriate non-disclosure, confidentiality,

and appropriate code-of-conduct agreements. Contractual agreements shall state responsibilities for information security as needed. Employees and relevant third-parties shall follow all [Company] security policies.

Management Responsibilities

Management shall be responsible for ensuring that information security policies and procedures are 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.

Management shall consider excessive pressures, and opportunities for fraud when establishing incentives and segregating roles, responsibilities, and authorities.

Termination Process

Employee and contractor termination and offboarding 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.

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 [Company] information security policies shall be subject to the [Company] progressive disciplinary process, up to and including termination of employment or contract.

Exceptions

Requests for an exception to this policy must be submitted to the CEO or [designated HR employee] for approval.

Violations and Enforcement

Any known violations of this policy should be reported to the CEO and [designated HR employee]. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance

Information Security Policy

Policy Owner: [Name]

Effective Date: [Date]

Purpose: The purpose of this policy is to communicate our information security policies and outline the acceptable use and protection of [Company]'s information and assets. These rules are in place to protect customers, employees, and [Company]. Inappropriate use exposes [Company] to risks including virus attacks, compromise of network systems and services, financial and reputational risk, and legal and compliance issues. Risk mitigation is outlined in [Company]'s Risk Management policy.

The [Company] "Information Security Policy" consists of this policy and all [Company] 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 [Company] business or interact with internal networks and business systems, whether owned or leased by [Company], the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at [Company] and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with [Company] policies and standards, and local laws and regulations.

This policy applies to employees, contractors, consultants, temporaries, and other workers at [Company], including all personnel affiliated with third parties. This policy applies to all [Company]-controlled company and customer data as well as all equipment, systems, networks and software owned or leased by [Company].

Policy: This Information Security Policy is intended to protect [Company]'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 [Company]. 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 [Company] 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.

Security Incident Reporting

All users are required to report known or suspected security events or incidents, including policy violations and observed security weaknesses. Incidents shall be reported immediately or as soon as possible by whatever means are quickest to leadership, whether it be by email to [company email] or slack, text, or call to the CEO and [designated security lead] .

In your communications you must describe the incident or observation along with any relevant details.

Whistleblower Anonymous Fraud Reporting

Our Whistleblower Policy is intended to encourage and enable employees and others to raise serious concerns internally so that we can address and correct inappropriate conduct and actions. It is the responsibility of all employees to report concerns about violations of our code of ethics or suspected violations of law or regulations that govern our operations.

It is contrary to our values for anyone to retaliate against any employee or who in good faith reports an ethics violation, or a suspected violation of law, such as a complaint of discrimination, or suspected fraud, or suspected violation of any regulation. An employee who retaliates against someone who has reported a violation in good faith is subject to discipline up to and including termination of employment.

Anonymous reports may be submitted via the form here: [Link to anonymous reporting form]

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 email 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 a device is prohibited.

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

- Devices must be locked with a password (or equivalent control such as biometric)
- Protected screensaver or screen lock after 15 mins.
- Devices must be locked whenever left unattended
- Users must report any suspected misuse or theft of a mobile device immediately to the CEO
- 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 resources (such as file shares and 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

Clear Screen Clear Desk: Users shall not leave confidential materials unsecured on their desk or workspace, and will ensure that screens are locked when not in use.

Remote Access Policy

Laptops and other computer resources that are used to access the [Company] network must adhere to the following standards:

- To ensure mobile devices do not connect a compromised device to the company network, Antivirus policies require the use and enforcement of client-side antivirus software
- Laptops and other computer resources other than mobile phones must be enrolled in [Company]'s Mobile Device Management infrastructure
- Antivirus software must be configured to detect and prevent or quarantine malicious software, perform periodic system scans, and have automatic updates enabled
- Users must not connect to any outside network without a secure, up-to-date software firewall configured on the mobile computer

- Users are prohibited from changing or disabling any organizational security controls such as personal firewalls, antivirus software on systems used to access [Company] 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 multi-factor authentication (MFA)
- Unauthorized remote access technologies may not be used or installed on any [Company] system
- Access is prohibited from public computer systems

Acceptable Use Policy

[Company] proprietary and customer information stored on electronic and computing devices, whether owned or leased by [Company], the employee or a third party, remains the sole property of [Company] for the purposes of this policy. Employees and contractors must ensure through legal or technical means that proprietary information is protected in accordance with the Data Management Policy. The use of Cloud Storage (Drive, Notion) for business file storage is required for users of laptops or company issued devices. Storing important documents on the file share is how you "backup" your laptop.

You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of [Company] proprietary information or equipment. You may access, use or share [Company] proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties. Employees are responsible for exercising good judgment regarding the reasonableness of personal use of company-provided devices.

For security and network maintenance purposes, authorized individuals within [Company] may monitor equipment, systems and network traffic at any time. [Company] reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities with properly documented Management approval. Under no circumstances is an employee of [Company] authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing [Company] resources or while representing [Company] in any capacity.

The list below is not exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

- 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 [Company].
- 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 [Company] or the end user does not have an active license
- Accessing data, a server, or an account for any purpose other than conducting [Company] business, even if you have authorized access, is prohibited
- Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws, is illegal. The appropriate management shall be consulted prior to export of any material that is in question
- Introduction of malicious programs into the network or systems (e.g., viruses, worms, Trojan horses, email bombs, etc.)
- 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
- Using a [Company] computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws
- Making fraudulent offers of products, items, or services originating from any [Company] account
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties
- 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, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes
- Port scanning or security scanning is expressly prohibited unless prior notification to the [Company] engineering team is made

- 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
- Circumventing user authentication or security of any host, network, or account
- Introducing honeypots, honeynets, or similar technology on the [Company] network.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack)
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, by any means
- Providing information about, or lists of: [Company] employees, contractors, partners, or customers to parties outside [Company] without authorization

Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company and act accordingly. The following activities are strictly prohibited, with no exceptions:

- 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)
- Any form of harassment via email, telephone, or texting, whether through language, frequency, or size of messages
- Unauthorized use, or forging, of email header information
- 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
- Creating or forwarding "chain letters", "Ponzi", or other "pyramid" schemes of any type
- Use of unsolicited email originating from within [Company] networks or other service providers on behalf of, or to advertise, any service hosted by [Company] or connected via [Company]'s network

Information Security Roles and Responsibilities

These are core information security responsibilities that every organization should assign to specific individuals or roles. Fill in the job title or person's name for each category based on your company structure. Some roles may be combined or delegated depending on size and resources.

The **CEO** shall be responsible for the following:

- Oversight of cyber-risk and internal control for information security, privacy and compliance
- Approves Capital Expenditures for Information Security and Privacy programs and initiatives
- Oversight over the execution of the information security and privacy risk management program and risk treatments
- Aligns Information Security and Privacy Policy and Posture based on [Company]'s mission, strategic objectives and risk appetite
- Responsible for oversight over third-party risk management process
- Responsible for review of vendor service contracts

The **[senior technical leader / CISO / IT Director]** shall be responsible for the following:

- Oversight over the implementation of information security controls for infrastructure, IT processes, and software development processes.
- Responsible for the design, development, implementation, operation, maintenance and monitoring of IT security controls and commercial cloud infrastructure.
- Oversight over Identity Management and Access Control processes
- Responsible for oversight over policy development related to systems and software under their control
- Responsible for implementing risk management in the development process aligned with company goals

Various **System Owners** shall be responsible for the following:

- Maintain the confidentiality, integrity and availability of the information systems for which they are responsible in compliance with [Company] policies on information security and privacy
- Approval of technical access and change requests for non-standard access to systems under their control

Additional Policies and Procedures Incorporated by Reference

Personnel are responsible for reading and complying with all policies relevant to their roles and responsibilities.

- **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, Disaster Recover, and Incident Response Plan**: To prepare [Company] in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame, as well as policy and procedures for suspected or confirmed information security incidents.
- **Cryptography Policy:** To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
- **Data Management Policy:** To ensure that information is classified and protected in accordance with its importance to the organization.
- **Human Resource Policy:** To ensure that employees and contractors meet security requirements, understand their responsibilities, and are suitable for their roles.
- **Operations Security Policy**: To ensure the correct and secure operation of information processing systems and facilities.
- **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 [Company]'s information security risks in order to achieve the company's business and information security objectives.
- **Third-Party Management Policy:** To ensure protection of the organization's data and assets that are shared with, accessible to, or managed by suppliers, including external parties or third-party organizations such as service providers, vendors, and customers, and to maintain an agreed level of information security and service delivery in line with supplier agreements.

Policy Compliance

[Company] will measure and verify compliance to this policy through various methods, including but not limited to ongoing monitoring, and both internal and external audits.

Exceptions

Requests for an exception to this policy must be submitted to the [Employee in charge of Information Security] for approval.

Violations

Any known violations of this policy should be reported to the [Employee in charge of Information Security]. 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.

Operations Security Policy

Policy Owner: [Name]

Effective Date: [Date]

Purpose: To ensure the correct and secure operation of information processing systems and facilities.

Scope: All [Company] information systems that are business critical and/or process, store, or transmit company data. This Policy applies to all employees of [Company] and other third-party entities with access to [Company] networks and system resources.

Policy: The policy is as outlined below.

Documented Operating Procedures

Both technical and administrative operating procedures shall be documented as needed and made available to all users who need them.

Change Management

Changes to the organization, business processes, information processing facilities, production software and infrastructure, and systems that affect information security in the production environment and financial systems shall be tested, reviewed, and approved prior to production deployment. All significant changes to in-scope systems and networks must be documented.

Change management processes shall include:

- Processes for planning and testing of changes, including remediation measures
- Documented managerial approval and authorization before proceeding with changes that may have a significant impact on information security, operations, or the production platform
- Advance communication/warning of changes, including schedules and a description of reasonably anticipated effects, provided to all relevant internal and external stakeholders
- Documentation of all emergency changes and subsequent review
- A process for remediating unsuccessful changes

Capacity Management

The use of processing resources and system storage shall be monitored and adjusted to ensure that system availability and performance meets [Company] requirements.

Human resource skills, availability, and capacity shall be reviewed and considered as a component of capacity planning and as part of the annual risk assessment process. Scaling resources for additional processing or storage capacity, without changes to the system, can be done outside of the standard change management and code deployment process.

Systems and Network Configuration, Hardening, and Review

Firewalls and/or appropriate network access controls and configurations shall be used to control network traffic to and from the production environment in accordance with this policy.

Production network access configuration rules shall be reviewed at least annually. Tickets shall be created to obtain approvals for any needed changes.

Protection from Malware

In order to protect the company's infrastructure against the introduction of malicious software, detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

Anti-malware protections shall be utilized on all company-issued endpoints. The anti-malware protections utilized shall be capable of detecting all common forms of malicious threats and performing the appropriate mitigation activity (such as removing, blocking or quarantining).

[Company] should scan all files upon their introduction to systems, and continually scan files upon access, modification, or download. Anti-malware definition and engine updates should be configured to be downloaded and installed automatically whenever new updates are available.

Known or suspected malware incidents must be reported as a security incident.
It is a violation of company policy to disable or alter the configuration of anti-malware

protections without authorization.

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.

Logging should meet the following criteria for production applications and supporting infrastructure:

- Log user log-in and log-out
- Logs must include user ID, IP address, valid timestamp, type of action performed, and object of this action.
- Logs must be stored for at least 30 days, and should not contain sensitive data or payloads

File Integrity Monitoring & Intrusion Detection

[Company] production systems shall be configured to monitor, log, and self-repair and/or alert on suspicious changes to critical system files where feasible.

Alerts shall be configured for suspicious conditions and engineers shall review logs on a regular basis.

Unauthorized intrusions and access attempts or changes to [Company] systems shall be investigated and remediated in accordance with the Incident Response Plan.

Control of Operational Software

The installation of software on production systems shall follow the change management requirements defined in this policy.

Technical Vulnerability Management

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities shall be

evaluated, and appropriate measures taken to address the associated risk. A variety of methods shall be used to obtain information about technical vulnerabilities, including vulnerability scanning, penetration tests, and review of external vendor alerts.

Supply chain security scanning is routinely performed on all [Company] code.

Penetration tests of the applications and production network shall be performed at least once every two years, and additional scanning and testing shall be performed following major changes to production systems and software.

The [IT and Engineering] departments shall evaluate the severity of vulnerabilities identified from any source, and if it is determined to be a risk-relevant critical or high-risk vulnerability, a service ticket will be created. [Company] assessed severity level may differ from the level automatically generated by scanning software or determined by external researchers based on [Company]'s internal knowledge and understanding of technical architecture and real-world impact/exploitability. Tickets are assigned to the system, application, or platform owners for further investigation and/or remediation.

Service tickets for any vulnerability which cannot be remediated within the standard timeline must show a risk treatment plan and planned remediation timeline.

Restrictions on Software Installation

Rules governing the installation of software by users shall be established and implemented in accordance with the [Company] Information Security Policy.

Information Systems and Audit Considerations

Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.

System Security Assessment & Requirements

Risks shall be considered prior to the acquisition of, or significant changes to, systems, technologies, or facilities. Where requirements are formally identified, any relevant security requirements shall be included. The acquisition of new suppliers and services shall be made in accordance with the Third-Party Management Policy.

The company shall perform an annual network security assessment that includes a review of major changes to the environment such as new system components and network topology.

Exceptions

Requests for an exception to this Policy must be submitted to the [designated IT or security employee] for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the CEO. 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.

Physical Security Policy

Policy Owner: [Name]

Effective Date: [Date]

Purpose: To prevent unauthorized physical access or damage to the organization's information and information processing facilities.

Scope: All [Company] offices and locations. This Policy applies to all employees of [Company], and to all external parties with physical access to [Company] owned or leased facilities.

Policy: The physical security policy is as outlined below.

Securing Offices, Rooms, & Facilities

Physical security for offices, rooms and facilities shall be designed and applied to protect from theft, misuse, environmental threats, unauthorized access, and other threats to the confidentiality, integrity, and availability of classified data and systems.

Protecting Against External & Environmental Threats

Physical protection against natural disasters, malicious attacks or accidents shall be designed and applied. Secure areas shall be monitored through the use of appropriate controls, such as intrusion detection systems, alarms, and/or video surveillance systems, where feasible. Visitor and third-party access to secure areas shall be restricted to reduce the risk of information loss and theft.

Working in Secure Areas & Visitor Management

Visitors, delivery personnel, outside support technicians, and other external agents shall not be permitted access to secure areas without escort and/or appropriate oversight. Third-parties in secure areas shall sign in and out on a visitor log and shall be escorted or monitored by [Company] personnel. [Company] personnel observing unescorted visitors should approach the visitor, confirm their status, and ensure they return to approved areas, or report the observation to the responsible authority as needed. External party access to

secure areas shall be confirmed with appropriate [Company] personnel prior to being granted access.

[Company] personnel providing access to external parties into secure areas are responsible for ensuring that the third-party personnel adhere to all security requirements, and are accountable for all actions taken by outsiders they provide with access. Visitors may be allowed to work unescorted provided that the [Company] sponsoring party can ensure that they will not have unauthorized access to [Company] information systems, networks, or data.

Supplier, Vendor, and Third-Party Security

Suppliers, vendors, and third-parties shall comply with [Company] physical security and environmental controls requirements. [Company] shall assess the adequacy of third-party physical security controls as part of the vendor management process, in accordance with the Third-Party Management Policy.

Exceptions

Requests for an exception to this Policy must be submitted to the CEO for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the CEO. 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.

Risk Management Policy

Policy Owner: [Name]

Effective Date: [Date]

Purpose: To define actions to address [Company] information security risks and opportunities. To define a plan for the achievement of information security and privacy objectives.

Scope: This policy applies to all employees of [Company] and to all external parties, including but not limited to [Company] consultants and contractors, business partners, vendors, suppliers, outsource service providers, and other third party entities with access to [Company] networks and system resources. This policy also includes all [Company] IT systems that process, store or transmit confidential, private, or business-critical data.

Policy: This policy outlines risks that could affect the medium to long-term goals of [Company] as risks that will be encountered in the day-to-day delivery of services. [Company] risk management systems and processes will be targeted to achieve maximum benefit without increasing the bureaucratic burden and ultimately affecting core service delivery to the organization. [Company] will therefore consider the materiality of risk in developing systems and processes to manage risk.

Risk Management Statement

Inadequate IT risk management exposes [Company] to risks including compromise of [Company] or customer network systems, services and information, cyber-attacks, contractual, or legal issues. [Company] 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 it achieves its stated business plan aims and objectives.

Risk Management Strategy

[Company] has developed processes to identify those risks that will hinder the achievement of its strategic and operational objectives. [Company] 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. [Company] ensures the risk management strategy and policy are reviewed regularly and that internal audit functions are responsible for ensuring: The risk management policy is applied to all applicable areas of [Company]. The risk management policy and its operational application are regularly reviewed. Non-compliance is reported to appropriate company officers and authorities.

Practical Application of Risk Management

[Company] has adopted a standard format for use in the identification of risks, their classification, and evaluation.

The format is based on the following NIST and ISO standards and frameworks:

- ISO 27005
- NIST 800-30
- NIST 800-37

Risks are assessed and ranked according to their impact and their likelihood of occurrence. A formal Risk Assessment, and network penetration tests, will be performed at least once every two years and shall take into consideration the results of any technical vulnerability management activities performed in accordance with the Operations Security Policy.

Risk Categories

Some risks are within the control of [Company] whilst others may be only to a lesser Degree. [Company] will therefore take an approach that will identify those risks and classify the risks according to the following categories:

- Reputational
- Contractual
- Regulatory/Compliance
- Economic/Financial
- Fraud
- Privacy
- Environmental & Sustainability
- Impact on People
- Operational Capacity

Each risk will be assessed as to its likelihood and impact. Both impact and likelihood can be assessed as Critical, High, Medium, Low.

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 organizational and customer information, personally identifiable information (PII), or business information systems.

For all risk inputs such as risk assessments, vulnerability scans, penetration test, bug bounty programs, etc., [Company] management shall reserve the right to modify 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, Treatment, & Tracking

Risk will be prioritized and maintained in a risk register where they will be prioritized and mapped using the approach contained in this policy. The following responses to risk should be employed:

- Modify: [Company] takes actions or employs strategies to reduce the risk.
- Accept: [Company] 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: [Company] 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 [Company] or insurance may be appropriate for protection against financial loss.
- Avoid: the risk may be such that [Company] could decide to cease the activity or to change it in such a way as to end the risk.

Where [Company] chooses a risk response other than "Accept" or "Avoid" it shall develop a Risk Treatment Plan.

Risk Management Procedures

The procedure for managing risk will meet the following criteria:

- [Company] will maintain a Risk Register and Treatment Plan.
- Risks are ranked by 'likelihood' and 'severity/impact' as critical, high, medium, and low.
- Overall risk shall be determined through a combination of likelihood and impact.

Risk Roles & Responsibilities

The **CEO** is ultimately responsible for the acceptance and/or treatment of any risks to the organization.

Exceptions

Requests for an exception to this Policy must be submitted to the CEO for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the CEO. 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.

Third-Party Management Policy

Policy Owner: [Name]

Effective Date: [Date]

Purpose: To ensure protection of the organization's data and assets that are shared with, accessible to, or managed by suppliers, including external parties or third-party organizations such as service providers, vendors, and customers, and to maintain an agreed level of information security and service delivery in line with supplier agreements.

This document outlines a baseline of security controls that [Company] expects partners and other third-party companies to meet when interacting with [Company] Confidential data.

Scope: All data and information systems owned or used by [Company] that are business critical and/or process, store, or transmit Confidential data. This policy applies to all employees of [Company] and to all external parties, including but not limited to [Company] consultants, contractors, business partners, vendors, suppliers, partners, outsourced service providers, and other third-party entities with access to [Company] data, systems, networks, or system resources.

Policy: Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented. For all service providers who may access [Company] Confidential data, systems, or networks, proper due diligence shall be performed prior to provisioning access or engaging in processing activities. Information shall be maintained regarding which regulatory or certification requirements are managed by or impacted by each service provider, and which are managed by [Company] as required. Applicable regulatory or certification requirements may include ISO 27001, SOC 2, PCI DSS, CCPA, GDPR or other frameworks, compliance standards, or regulations.

Security in Agreements

Relevant information security requirements shall be established and agreed upon with each supplier that may access, process, store, transmit, or impact the security of Confidential data and systems, or provide physical or virtual IT infrastructure components for [Company]. For all service providers who may access [Company] production systems, or who may impact the security of the [Company] production environment, written agreements shall be maintained that include the service provider's acknowledgment of their responsibilities for the confidentiality of company and customer data, and any

commitments regarding the integrity, availability, and/or privacy controls that they manage in order to meet the standards and requirements that [Company] has established in accordance with [Company]'s information security program or any relevant framework.

Third-Party Service Delivery Management Monitoring & Review of Third-Party Services

[Company] shall regularly monitor, review, and audit supplier service delivery. Supplier security and service delivery performance shall be reviewed at least annually for critical suppliers, as adjudicated by the CEO or [senior Ops or security leader].

Third-Party Risk Management

[Company] will ensure that potential risks posed by sharing Confidential data or providing access to company systems are identified, documented and addressed according to this policy. Risk management plays an integral part in the governance and management of the organization at a strategic and operational level. The purpose of a partner and third-party security policy is to ensure that partnerships and services achieve their business plan aims and objectives, and are consistent with [Company]'s requirements for information security. [Company] shall not share or transmit Confidential data to a third-party without first performing a third-party risk assessment and fully executing a written contract, statement of work or service agreement which describes expected service levels and any specific information security requirements.

Third-Party Security Standards

All third-parties must maintain reasonable organizational and technical controls as assessed by [Company].

Assessment of third-parties which receive, process, or store Confidential data or access [Company]'s resources shall consider the following controls as applicable based on the service provided and the sensitivity of data stored, processed or exchanged.

Information Security Policy

Third-parties maintain information security policies supported by their executive management,which are regularly reviewed.

Risk Assessment & Treatment

Third-parties maintain programs that assess, evaluate, and manage information and technology risks.

Operations Security

Third-parties implement commercially reasonable practices and procedures designed, as appropriate, to maintain operations security. Protections may include:

- Technical testing
- Protection against malicious software
- Network protection and management
- Technical vulnerability management
- Logging and monitoring
- Incident response
- Business continuity planning

Access Control

Third-parties maintain a technical access control program.

Human Resources

Third-parties maintain human resource policies and processes which include criminal background checks for any employees or contractors who access [Company] confidential information.

Compliance & Legal

[Company] shall consider all applicable regulations and laws when evaluating suppliers and third parties who will access, store, process or transmit [Company] confidential data. Third-party assessments should consider the following criteria:

- Protection of customer data, organizational records, and records retention and disposition
- Privacy of Personally Identifiable Information (PII)

Exceptions

Requests for an exception to this Policy must be submitted to the CEO for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the CEO. 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.