IS-1 General Information Security Policy

**1.1 Information Security Policy**

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

The company Chief Information Officer (“CIO”) is responsible for the Design, Development, Maintenance, Dissemination, and Enforcement of the items contained in this Policy Manual. At a minimum on a quarterly basis security and/ or compliance committee comprised of senior management and key personnel must discuss, evaluate and document security program ensuring strategic goal and objectives are continually being developed. At a minimum on an annual basis all policies must be reviewed, modified and/ or edited to meet necessary security standards. All policies must be signed and approved by authorized personnel.

Policies/ procedures must be accessible to employees for review at all times via internal intranet. Policies pertaining to positions must be reviewed and signed upon hire and on an annual basis by all employees.

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

**Purpose**

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

**Scope**

This Policy Manual applies to:

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

**Training**

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

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

All new hires are required to complete information security training, including appropriate incident response training for their role, as part of their new employee orientation process and annually thereafter. Training will be done within 60 days after the date the employee is hired. Ongoing training will include security and privacy requirements as well as training in the correct use of information assets and facilities.

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

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

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

III. once a year thereafter.

The organization will document that the training has been provided to all employees. All employees are required to acknowledge in writing their understanding of the Information Security Program which includes a Code of Conduct upon hire and annually thereafter.

**Clean Work Area Policy**

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

**Internet/Intranet Access and Use**

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

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

**Enforcement**

<COMPANY NAME> Management, under the explicit authority granted by the company CEO, retains the authority and responsibility to monitor and enforce compliance with this Policy Manual and other policies, standards, procedures, and guidelines. Internal independent audits must be conducted at least annually by authorized security personnel to ensure the information protection program is approved by senior management, communicated to stakeholders, adequately resourced, sufficiently budgeted, conforms to relevant legislation or regulations, and adjusted as needed to ensure the program continues to meet defined objectives.

Monitoring will include, but is not limited to: capturing and or filtering of hardcopy, magnetic, optical, or electronic data traffic; reviewing transmitted and/or stored e-mail, Instant Messaging, “texting”, chat, and/or other forms of messages; telephone and voice communication, files, and voicemail; maintaining activity log files; or reviewing the contents of storage facilities for inappropriate content or other actions determined to be harmful to the Company, customers, and/or affiliates. In addition, Internet and other network activity will be monitored. General Security Policy

Monitoring activities may be conducted on an on-going basis or on a random basis whenever deemed necessary by Management and may require investigating the use of the Company’s information resources. The company reserves the right to review any and all communications and activities without notice.

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

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

**Employee Sanctions**

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

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

**Corrective Action Procedure**

**Step 1: Verbal warning and counseling**

Step 1 creates an opportunity for the immediate supervisor to schedule a meeting with an employee to bring attention to an existing performance, conduct or attendance issue. The supervisor should discuss with the employee the nature of the problem or the violation of company policies and procedures. The supervisor is expected to clearly describe expectations and the steps the employee must take to improve performance or resolve the problem.

**Step 2: Formal written warning**

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

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

**Step 3: Suspension and final written warning**

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

Depending on the seriousness of the infraction, the employee may be suspended without pay in full-day increments consistent with federal, state and local wage-and-hour employment laws. Non-exempt / hourly employees may not substitute or use an accrued paid vacation or sick day in lieu of the unpaid suspension. Due to Fair Labor Standards Act (FLSA) compliance issues, unpaid suspension of salaried/exempt employees is reserved for serious workplace safety or conduct issues. HR will provide guidance so that the discipline is administered without jeopardizing the FLSA exemption status. Pay may be restored to the employee if incident/infraction investigation absolves the employee.

**Step 4: Recommendation for termination of employment**

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

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

**Performance and Conduct Issues Not Subject to Progressive Discipline**

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

**Documentation**

All copies of the progressive discipline documentation, including all PIPs will be placed in the employee’s official personnel file by HR. The employee will be given copies and will be asked to sign HR’s copies attesting to his or her receipt and understanding of the corrective actions outlined in these documents.

***APPENDIX A***

**Code of Conduct**

**Purpose**

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

**Who must follow the Code?**

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

**Who to ask about the Code?**

If you have a question or concern about the Code, be proactive and contact your manager or the Compliance team. You can also submit a question or raise a concern regarding a suspected violation of our Code (or any other <COMPANY NAME> policy) to your manager.

**No retaliation**

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

**Code of conduct**

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

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

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

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

**Quality Work Environment**

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

**1. Equal opportunity employment**

Employment at <COMPANY NAME> is based solely upon individual merit and qualifications directly related to professional competence. We strictly prohibit unlawful discrimination or harassment on the basis of race, color, religion, veteran status, national origin, ancestry, pregnancy status, sex, gender identity or expression, age, marital status, mental or physical disability, medical condition, sexual orientation, or any other characteristics protected by law. We also make reasonable accommodations to meet our obligations under laws protecting the rights of the disabled.

**2. Harassment, discrimination, and bullying**

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

**3. Drugs and alcohol**

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

**4. Safe workplace**

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

**Avoid Conflicts of Interest**

As <COMPANY NAME> employees, we should avoid conflicts of interest and circumstances that reasonably present the appearance of a conflict of interest, especially if it would create an incentive for you or present the appearance of an incentive for you, (whether directly or indirectly). Here is list of areas where conflicts of interest often arise:

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

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

**Preserve Confidentiality**

Throughout its lifecycle, all nonpublic information that is processed, transmitted, and/ or stored by <COMPANY NAME> must be protected in a manner that is consistent with our contractual and legal requirements and reasonable and appropriate for the level of sensitivity, value, and risk associated with *Nonpublic* information (please see Data Classification System). Information that contains data elements from multiple classifications must be protected at the highest level of information represented. For example, a document that contains *Nonpublic* and *Public* information must be treated as *Nonpublic* information. Nonpublic information must be secured against disclosure, modification, and access by unauthorized individuals. Therefore, the information must be:

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

**Information Security**

You’re responsible for using <COMPANY NAME>’s computer resources properly – especially with regard to information security – and you need to be thoroughly familiar with <COMPANY NAME>’s Information Security policies and procedures.

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

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

**Protect <COMPANY NAME>’s Assets**

**1. Intellectual property**

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

Likewise, respect the intellectual property rights of others. Inappropriate use of others’ intellectual property may expose <COMPANY NAME> and you to criminal and civil fines and penalties. Seek advice from the Legal team before you solicit, accept, or use proprietary information from individuals outside the company or allow them obtain access to <COMPANY NAME> proprietary information. You should also check with the Legal team if developing a product feature that uses content not belonging to <COMPANY NAME>.

**2. Company Equipment**

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

**3. The Network**

<COMPANY NAME>’s network, software, and computing hardware are a critical aspect of our company’s physical property and intellectual property. Follow all security policies diligently. If you have any reason to believe that our network security has been violated – for example, you lose your laptop or think that your network password may have been compromised – promptly report the incident to your manager. For more information, consult <COMPANY NAME>‘s Information Security Policy.

**4. Physical Security**

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

**Ensure Financial Integrity and Responsibility**

Financial integrity and fiscal responsibility are core aspects of corporate professionalism. Each person at <COMPANY NAME> has a role in making sure that money is appropriately spent, our financial records are complete and accurate, and internal controls are honored. This is applicable every time that we hire a new vendor, expense something to <COMPANY NAME>, or sign a new business contract.

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

**Obey the law**

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

**Policy Compliance**

**Compliance Measurement**

The Compliance team will verify compliance with this Code through various methods (e.g. periodic manager reviews, tool reports, internal and external audits, and employee feedback).

**Exceptions**

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

**Non-Compliance**

Any employee who violates this Code may be subject to disciplinary action, up to and including termination of employment in addition to any civil and criminal liability.

**Your Annual Acknowledgment of the Code of Conduct**

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

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