Cybersecurity and IT Policy

Ericius Security

01 March 2022

Contents

1 Cybersecurity and IT Policy

1.1 Policy Statement

COMPANYshall adopt and follow well-defined and time-tested plans and procedures and layout cybersecurity objectives to meet business objectives and ensure continuity of operations and processes.

1.2 Purpose

1. The purpose of this policy is to establish cybersecurity guidelines that ensure our ability to accomplish our mission: TEMP MISSION STATEMENT.

2. Put another way; this program allows us to go to market and win by enabling us to create and capture more revenue, reducing cybersecurity risk, which reduces expected loss from damage to reputation and cost to recover.

3. This cybersecurity policy explains why we need to proactively steward information, technology, and people. We build and maintain our security program because it enables us to build trust, confidence, and goodwill within the market and with our teammates and partners. Further, we specifically outline the program standards to which we aspire and outline the processes by which we achieve those standards such that we can both capture more revenue in the market and reduce overall risk to the organization.

1.3 Scope

1. This policy applies to COMPANY, our employees, our applicable third parties, our technology use, our IT infrastructure, our computing resources, our networks, our information, and our data, and any of the above categories that we could be perceived as being stewards over.

2. The scope is limited by applicable legal and contractual obligations where required.

1.4 Enforcement and Expectation of Compliance

Any user or person bound to this policy that is found to have violated these policies may be subject to disciplinary action, including termination of employment, contract, or another arrangement.

1.5 Roles and Responsibilities

1. You - As a COMPANYstaff member or applicable third-party, you are an integral part of our security program. You maintain appropriate levels of access and privileges and defend the COMPANYwith constant vigilance and discipline. You are required to keep the appropriate authorities informed of technology adds, changes, and reductions and report vulnerabilities and gaps. We cannot protect your needs if we are unaware that you have something you need us to protect.

2. CEO - The CEO is responsible for living cybersecurity fundamentals and setting the standard which empowers the team to drive the program. The CEO establishes priorities and goals for COMPANY, which the cybersecurity program and policies support.

3. CISO - The CISO leads the cybersecurity department and is responsible for reducing business risk through the judicious application of training, auditing, compliance, governance, and communication across COMPANYand is responsible for establishing all cybersecurity policies subordinate to this one, including but not limited to the policies attached to this policy as appendices. When applicable, the CISO receives policy and program guidance from the Head of Internal Audit. The CISO role may, from time to time, include third parties such as consultants or virtual CISOs.

4. Legal Counsel - COMPANYlegal counsel provides a checkpoint for all security programs and ensures that areas such as data retention or emergency mode operations comply with legal and regulatory requirements. They are a primary stakeholder during some forms of incident response. They are the direct voice of the COMPANYbetween internal stakeholders, any government entity, and partner, client, or user communications. Often, the Legal Counsel works closely with the external (public) communications team during an incident.

5. Head of Internal Audit - The head of internal audit is responsible for establishing COMPANY's top-level policies, including this policy, and for reviewing and ensuring the proper implementation of COMPANY's top-level policies and all policies nested underneath them.

6. IT Team - Execute change in harmony with other stakeholders identified here to maintain the technical ability to execute COMPANYoperations. Support the needs of COMPANY's other staff, lead the change control process, and govern identity and access management through the organization. The IT team includes badged employees and contracted or third-party service providers who directly manage COMPANY's assets and infrastructure.

7. Office Manager - Responsible for physical access management, key control, and daily security. The office manager coordinates responses to physical incidents and notifies cybersecurity and IT personnel.

8. Privileged Users - Users of COMPANYIT and computing assets with administrative or increased access and permissions. COMPANYplaces a high degree of trust and confidence in its privileged users because they have access to more information and resources than other users and can grant others access to information and resources.

9. Third-Party Stakeholders - People or entities outside the organization that require access to COMPANY's information. Those stakeholders, as applicable, must sign proper authorizations such as non-disclosure agreements (NDAs/MNDAs), service agreements (SLAs, GLAs, etc.), and Business Associate Agreements (BAAs) when applicable before receiving privileged access. They are required to maintain the same levels of diligence to protect the confidentiality, integrity, and availability of our information, systems, and resources.

10. See associated RACI Charts, process documents, and personnel documents that define roles and responsibilities more granularly here: LINK_TO_RACI_DOCS
    - Note: RACI stands for Responsible, Accountable, Consult, and Inform. RACI documents are used to outline who owns what portions of processes and how to process information is communicated.

1.6 Terms

Asset - Including but limited to any intellectual property, information, data, physical or virtual property, equipment, software, service, or platform owned, operated, maintained or leased by COMPANY. In some contexts, this could include personal devices that have access to COMPANYassets.

1.7 Policies

1. COMPANY's Head of Internal Audit establishes this Cybersecurity and IT policy and delegates responsibility for all policies nested under it, such as the appendices attached herein.
2. COMPANYstrives not just to comply with regulatory frameworks—such as PCI and GDPR where applicable—but to improve and sustain its operations and ability to serve clients and users through deliberate risk-management. To this extent, we have an ongoing cybersecurity and risk-management program and will continue to apply and mature it both in scope and in practice.
3. We will employ countermeasures that include but are not limited to:
   a) Setting program standards
   b) Risk identification and classification
   c) Security training
   d) Identity management and identity-focused security
   e) Change control
   f) Judicious use of the principle of least privilege (applied zero trust)
   g) A focus on SaaS-based applications
   h) Deliberate management of third-party risk
   i) Securing communications, data, information, infrastructure, systems, endpoints, and owned, leased, or open-sourced platforms.
   j) Out-of-band communications
   k) Information classification, retention, and disposal
   l) External audit, assessment, and testing when and where applicable (usually annually)
   m) Asset, Vulnerability, and Patch Management
   n) Incident Response and Incident Management
   o) Log and Event Management and Retention
   p) Our strategy is simple. As Dustin Wilcox says: "Minimize the Attack Surface, Complicate Unauthorized Access, Rapidly Detect, Respond to, and Contain Incidents."

1.8 Exceptions

1. Deviations from or exceptions from these policies shall be submitted to the CISO and IT Team for approval and documentation.

2. The CISO and IT Team maintain a repository of approved exemptions and associate risk here: LINK_TO_EXCEPTIONS_REGISTRY

3. Note: Access to the exemption repository is controlled based on role and need to know. The link will not work for you without either.

1.9 Documentation and Control

1. Documents
   a) This Cybersecurity and IT policy document, all policies or documents contained or referenced herein, and all COMPANYpolicies shall be controlled. Version control will be applied to distinguish current versions from all previous revisions. All such policies and documents will be retained in digital form for two years from their last effective date unless other authorities mandate the period.
   b) After two years from the last effective date of a policy or document, all physical or digital copies of a document or policy will be securely destroyed by shredding and/or secure deletion except when a legal hold or other relevant exception is in place.
   c) This policy does not apply to log retention, which is governed by a separate policy.

2. Records
   a) Records generated as part of the Cybersecurity and IT policy or a policy contained or referenced herein shall be retained for two years. Department leads will own their respective policies and will audit yearly. Records shall be encrypted at rest and in transit.
   b) To maintain compliance, specific records with a longer retention rate will be maintained for the period outlined by the appropriate laws and statutes. These include but are not limited to legal actions, insurance settlements, and tax records that have varying retention requirements.

3. Distribution and Maintenance
   a) The Cybersecurity and IT policy is not a public document. However, it may be provided to all badged stakeholders and a limited set of third parties when applicable. This availability includes all changes and revisions. The Head of Internal Audit, DPLO, and or CISO will be responsible for this document and its contents.
   b) The CISO and IT Team maintain a repository of approved policies, both current and historical here: LINK_TO_DOCS_AND_POLICY

1.10 Subordinate Policies (Appendices)

A. Information Classification, Handing, and Retention Policy

B. Incident Management Policy and Process

C. Asset Management Policy

D. Acceptable Use Policy

E. Change Management and Change Control Policy

F. Remote Working Policy - See Employee Handbook

G. Security Awareness Policy and Process

H. Business Continuity Policy and Plan

I. Technical Security Policy

J. Reputation Management

K. System Lifecycle Management

2 Appendix A: Information Classification, Handling, and Retention Policy

2.1 OVERVIEW AND PURPOSE

1. COMPANY shall adopt and follow well-defined and time-tested plans and procedures to ensure that sensitive or critical information is classified correctly and handled according to COMPANY's policies. The purpose of this policy is to help people understand what information may be used where and shared with whom and utilize that restriction to protect from unauthorized use and disclosure. This policy helps to facilitate how the COMPANY team identifies information to support routine disclosure and active dissemination of information, which also helps protect COMPANY's intellectual property.

2. This allows COMPANY to maintain continuous business objectives properly steward information on behalf of relevant parties.

3. Information is considered a primary asset for COMPANY. COMPANY uses multiple types of information assets, and the sensitivity and handling requirements of these information assets may vary.

2.2 Scope

This policy applies to entities outlined in the Cybersecurity and IT Policy base document. Specifically, this document outlines information and data assets.

2.3 Enforcement

See enforcement clause in the Cybersecurity and IT Policy.

2.4 Roles and Responsibilities

The CISO, DPLO, Head of Internal Audit, or equivalent person designated in writing is responsible for maintaining this policy in conjunction with appropriate other stakeholders such as the Legal Counsel. This role is accountable for proper implementation of the Information Classification and Handling Policy with various other department leads assuming responsibility for implementing the policy within their respective departments.

2.5 Acronyms

None for this policy

2.6 Policy

Privacy: This policy inherits its privacy from the base policy. Portions of this policy may, by exception, be held at a higher, more restrictive classification level and stored separately in accordance with access control policies as governed by that more restrictive classification level.

2.7 Classification Categories

1. COMPANY categorizes information into three classes: Public, Internal, and Confidential.
    a) Public - Definition: Information or assets intended for disclosure to or interaction with the public or that, if disclosed, pose no risk or damage to COMPANY.
        i. Public information includes information assets that do not have any confidentiality or regulatory requirements, or that can be disseminated to the public.
        ii. Examples include press releases, annual financial reports in accordance with compliance, marketing material, social media, and COMPANY's website.
    b) Internal - Definition: Information or assets that are not intended for public release but do not necessarily pose a significant risk or damage to COMPANY if released.
        i. Internal information includes information necessary for the organization and operation of COMPANY that is not necessarily confidential or information that can be circulated freely within all offices or departments in COMPANY but not necessarily the public.
        ii. Examples include personnel assignments, office orders, internal circulars, movement of personnel or equipment, or invoices.
    c) Confidential - Definition: Information or assets that pertain to the specific needs of the project, team, department, or business process or that pose a significant risk or damage to COMPANY if improperly disclosed.
        i. Confidential information includes information necessary for the business operations of departments or units, information that cannot be freely circulated within COMPANY, PII or PCI data, sensitive or proprietary information, and intellectual property that cannot be publicly disclosed except then directed by law, regulation, or legal order. Confidential information shall be restricted to need-to-know (an element of least privilege) such as those entities deeply associated with a project or business process. Access must be backed up and archived. It must be encrypted when transmitted or password-protected when encryption is not possible. It must also be backed up and archived when stored.
        ii. Examples include any information that would reduce COMPANY's ability to go to market and win, such as business strategy, plans for mergers or acquisition, PCI data, personnel files, service or other agreements, or other techniques or procedures not appropriate for public release.
    d) Confidential: Special, Related to XYZ: This is a sub-category of confidential that requires special handling potentially for client, compliance, or legal reasons outside of standard Confidential categories. Further definitions should be stored at a separate classification level than in this document.

2.8 Secure Handling of Information Assets

1. All information will be labeled according to its classification label in the header and footer of the document and clearly within the file name. In the case of physical storage media, it will be physically labeled with the highest level of information stored therein.

2. Some classification levels may require approval from the CISO, CEO, or legal counsel prior to transmission.

3. Restrict mailing and/or shipment of confidential information through only trusted mail services or couriers who must show authentication.

4. Store hard copy confidential information behind double lock and key.

5. Hard copy confidential information must be shredded at the end of life.

6. Take prudent cautions to prevent unauthorized personnel from accessing higher levels of restricted information.

7. Limit access control both by role and by person/entity.

8. Similarly treat confidential information as you would with both chains of custody and custodial responsibility.

9. Encrypt spooled data and validate user identity and permission prior to printing.

10. Limit distribution to "need to know" and "need to use."

11. Review persona and entity access monthly and at the end of major project phases.

12. The approval authority for downgrading an information asset's classification level resides with department leads, and when a classification level is in question, department leads are to consult with the owner of this policy, legal counsel, and or other executive stakeholders.

13. See associated charts, process documents, and controls more granularly here: LINK_TO_INFO_INVENTORY

2.9 Classification by Aggregation

1. Aggregating data and or information can change the classification level of that data. Converting data into information can change the classification of this newly created information asset. This is because information aggregation both represents an intellectual property base and can provide insights into the COMPANY's internal workings that could cause the COMPANY to lose in a competitive market.

2. When information is aggregated, it will, at a minimum, be classified at the highest level amongst all the information aggregated. For example, when information of internal classification is aggregated with information of confidential classification, the aggregated information is controlled as CONFIDENTIAL.

3. If several items at the same classification level are aggregated, the aggregated information will instead be classified as one level higher than the information aggregated. For example, several pieces of internal information aggregated into one document will be controlled as confidential.

3 Appendix B: Incident Management Policy and Process

3.1 Overview and Purpose

The Purpose of this policy is to ensure that information security increases our ability to win in the market and against our competition by effectively identifying, responding to, and managing information security incidents.

3.2 Scope

This policy applies to entities outlined in the Cybersecurity and IT Policy base document.

3.3 Enforcement

See enforcement clause in the Cybersecurity and IT Policy.

3.4 Roles and Responsibilities

1. CISO or other person designated in writing:
   a) Responsible for the proper implementation of the Incident Management Policy and Process
   b) Leads all aspects of response to an incident and is the primary source of truth and communication within the organization and coaches external communicators before breach disclosure to third parties. The CISO also leads incident response exercises and communicates the plan to senior leaders within the organization.
2. Office Manager - Keeps non-essential personnel from interfering with breach response.
3. IT Manager - Keep CISO informed of incidents.

3.5 Acronyms

1. IRT - Incident Response Team
2. PACE Plan - A plan to cover the Primary, Alternate, Contingency, and Emergency modes of accomplishing a particular task or action. The purpose of the PACE Plan is to provide the means to contact the people needed during an emergency to take the appropriate immediate action to respond to an emergency.
3. MTTR - Mean time to Resolution
4. IRT - Incident Response Team
5. CAL OES - California Governor's Office of Emergency Services. They have a good template, and we borrowed from it as the starting point for this document. They get credit for inspiration!
6. SUNY Broome - Another public-domain resource that we need to credit!

3.6 Policy

1. Incident Response Team
2. a) The following departments or sections will provide a point of contact who is available on a 24/7 basis to assist with any security incident that occurs:
    i. Facilities Manager or Physical Security Office
        A. Finance
        B. Legal Counsel
        C. Operations
        D. Technology
        E. Information Technology
        F. CISO
        G. Public Affairs, Marketing, or Communications
        H. Internal Audit
        I. Governance and Compliance
        J. Other departments as required
    b) If the appointed contact is not available, the department or section lead becomes the assisting party until another member of their department or section is replaced.
    c) A list of contact information is available here: LINK_TO_IRT_STAKEHOLDERS
3. Incident Response Team Notification
4. In collaboration with other departments, the information security team will establish a PACE plan for notifying all members, participants, or stakeholders of an incident response team in case of a security incident. Stakeholders may include third parties such as an outsourced SOC, IR team, MSSP, etc.
5. All potential members, participants, or stakeholders of an IRT will be familiar with the notification PACE plan and have appropriate personnel prepared to utilize any applicable services indicated.
6. Each department contributing a member to the IRT will establish an alias, distribution list, or equivalent that complies with the PACE Plan and notifies the appropriate individual assigned to IRT duty in case of an IRT notification.
7. The IRT Notification PACE Plan can be found here: LINK_TO_PACE_PLAN
8. Incident Response Team Communications
    a) According to a PACE Plan, the incident response team will establish an operations center and connect with communications tools.
    b) A physical operations center will include ample seating, tools for collaboration and presentation, and at least one computer workstation with access to a high-speed internet connection to connect remote participants virtually.

c) A virtual operations center will enable remote participants to communicate, present information and multi-media, and form semi-private collaboration spaces such as breakout rooms.

d) The IRT PACE Plan can be found here: LINK_TO_PACE_PLAN.

9. External Points of Contact - The information security department will maintain the following points of contact and make them available to the IRT:
   a) MSP
   b) MSSP
   c) Internet Service Provider
   d) Local FBI
   e) Local Law Enforcement's Computer Crime Department
   f) Local CIRT or FIRST
   g) Web Host
   h) Other Third-Party providers
10. Events and Incidents
    a) COMPANY will use the following definitions of events and incidents following the definitions in NIST 800-61 rev 2:
    b) Event - Any observable occurrence in a system or network, such as a user requesting a web page or a firewall blocking a connection attempt.
    c) Adverse event - an event with a negative consequence like a system crash or unauthorized use of system privileges
    d) Incident - a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. This may include such actions as the threat of or actual use of a Denial of Service (DoS) attack or Distributed DoS (DDoS), or a user hosting illegal content on company resources.
11. Triage and Escalation
12. Not every event turns into an incident. When an event is reported, the first person in the reporting chain with authority to determine if an event meets the threshold of an incident must triage the event (or attempt to correlate seemingly unconnected events) and make a judgment or seek additional information. That person must then document their decision in the appropriate register for tracking.
13. Tracking and reports
    a) When an incident occurs, COMPANY will assign the incident a category and track the incident in accordance with the process section of this appendix. When tracking or reporting, maintain the following information based on NIST 800-61 rev two and US-CERT Guidelines:
       i. The incident category and tracking number
       ii. The assessed functional impact

iii. The assessed information impacts

iv. The date and time that the activity was detected and the date and time the activity occurred

v. The number of systems, records, or users impacted.

vi. The network and physical location or identification of systems, records, or users impacted.

vii. The points of contact for additional follow-up

viii. The attack vector or root cause (as known/available)

ix. The associated indicators of compromise, including signatures or detection measures developed in relationship to the incident

x. The actions taken to mitigate the incident and recommended actions the client undertake

xi. Tracking is essential for reasons such as conducting post-mortem analyses, contributing to a lessons learned repository, identifying attack patterns that can expose insights about the team and the adversary.

14. Incident Categories - When categorizing incidents, use the following table:

Category	Name	Description	MTTR Goal
CAT A	Simulations	Used to annotate incidents created to test systems and simulate attackers	Not applicable
CAT B	Unauthorized Access or Compromised Asset	A person gains logical or physical access without permission to a client network, system, application, data, or other resource -Attempted or successful destruction, corruption, or disclosure of sensitive information or intellectual property -Compromised host, network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host (e.g. RAT)	1-3 hours
CAT C	Denial of Service	-An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources. -Either as victim of or participating in the DoS/DDoS	3 Hours
CAT D	Malware or Malicious Code	-A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host. -This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See CAT B)	12 Hours
CAT E	Inappropriate Access, Unlawful Activity	-Theft/ Fraud/ Human Safety/ Child Porn. Computer-related incidents of a criminal nature, potentially involving law enforcement. *NOTE	24 Hours
CAT F	AUP Violation	-A person violates acceptable use of any network or computer use policies.	24 Hours
CAT G	Reconnaissance, Scanning, or Attempted Access	-Any activity that seeks to access or identify a client computer, open ports, protocols, service, or any combination for later exploit. -This activity does not directly result in a compromise or denial of service.	72 Hours
CAT H	Uncategorized/Under Investigation	-Unconfirmed incidents that are potentially malicious or anomalous activity that warrants further review.	72 Hours

3.7 Categories of Functional Impact

The following define functional impact to COMPANY's systems or environments

Category	Definition
None	No impact on the COMPANY 's ability to go to market and win
Low	Minimal effect: COMPANY can still go to market but has reduced its competitive edge
Medium	COMPANY 's ability to go to market and win is in question
High	COMPANY is no longer able to go to market and win

3.8 Categories of Information Impact

The following table establishes information impact to COMPANY's systems or environments

Category	Definition
None	No impact to CIA or the ability to go to market and win
Suspected but not identified	A data loss or impact to availability is suspected, but no direct confirmation exists
Privacy Breach	Sensitive personally identifiable information (PII) of employees, customers, clients, or other third party was either accessed or exfiltrated. If you're unsure, ask your legal team!
Proprietary Breach	Proprietary information, such as intellectual property, was accessed or exfiltrated
Integrity loss	No longer able to trust either sensitive or proprietary information

3.9 Reporting

1. Employees who wish to report an observed incident can submit one by calling (XXX) XXX-XXXX), emailing reportingcompany.com or submitting a ticket at LINK_TO_TICKETING_SERVICE
2. The IRT will track the incident and provide periodic reports to COMPANY leadership.

3.10 Evidence Retention and Chain of Custody

1. Evidence or information collected will be tracked by quantity and description. People who have custodial responsibility must execute proper due diligence by securing evidence, limiting access, reporting the evidence under their control when and to whom applicable, and documenting that evidence. If a physical device, description will include:
   a) Manufacturer
   b) Model
   c) Serial Number
   d) If evidence is digital or a file, include:
   e) Filename
   f) File hash
   g) Modified, created, and accessed times
   h) File Size
   i) Physical media may also need to be protected with technology such as write blockers
   j) If evidence is a record of testimony or similar information, include:
   k) Name of interviewee
   l) Name of interviewer
   m) Location obtained
   n) Medium used
   o) Time collected
   p) Signature of both interviewee and interviewer

q) Records of testimony should only be used when legally required or advised by legal counsel.

r) When evidence is transferred from one party to another, chain of custody will be maintained regardless of the reason for transfer. A document must accompany the evidence that maintains the date and time of every transfer, who the evidence was transferred from, and who the evidence was transferred to. For each transfer, transferring and receiving parties will both record:

s) Date and time

t) Name

u) Organization/department

v) Signature

w) Purpose of custody change

3.11 Reporting template

1. COMPANY will track all incidents using LINK_TO_TICKETING_SERVICE and will establish a ticket format to capture all the information required by this policy.

2. Incident Response Tickets will have a category and template that indicates its high priority and is distinct from routine IT support or IT helpdesk tickets.

3. Should the ticketing system be unavailable for any reason, the following reporting template is provided as an alternative

Company Security Incident Report		
Incident Tracking Number		
Incident Category		
Functional Impact		
Informational Impact		
Dates and Times	Local	UTC
Detected		
Started		
Stopped		
Num. of affected systems, records, users		
Summary/Narrative of Incident		
Network location or identification of systems, records, or users impacted		
Attack vector or root-cause analysis		
Associated indicators of compromise		
Actions taken		
Recommended mitigations and/or follow-up actions		
Points of contact for follow-up		

3.12 Process

1. When an event is discovered, the individual who discovers it will report it to the appropriate entity such as the Security team, IT Committee, or CISO via phone, email, or trouble ticket.
2. The notification will immediately alert the information security team or security watch personnel, who will collect the following information and contact the reporter as needed: When notified of a security incident, immediately log the following:
   a) The caller/notifier's name
   b) Time of notification
   c) The notifier's contact information
   d) The nature of the incident (collect who, what, when, where, why)
   e) Equipment or persons involved
   f) Location of equipment or persons involved
   g) How the incident was detected
   h) When an event was first noticed indicating that an incident occurred
   i) Make an initial determination of the following or add details as appropriate:
   j) Is the equipment, system, or information impacted business critical?
   k) What is the severity of impact or potential category of incident?
   l) Name of the system being targeted, along with the operating system, IP address, and location
   m) Information about the origin of the attack, if possible including but not limited to IP address, domain name, specific ports or services, etc.
   n) Refer to the IT emergency contact list (Located here) and or PACE Plan for the affected department.
   o) Use the contact lists to determine both management personnel to be contacted and incident response personnel.
   p) Contact the appropriate incident response personnel using both email and phone messages.
   q) Note the time and manner of each contact
3. The staff member receiving notification will then list all additional parties who may discover the incident and collect their contact information. Parties to contact may include:
   a) Helpdesk
   b) The CISO
   c) Intrusion Detection monitoring personnel
   d) A system administrator
   e) A firewall administrator
   f) A business partner
   g) A manager

h) The security department or a security person

i) An outside source

4. List all parties to contact and determine the contact information for each. Each party should have at least one 24/7 point of contact identified. People outside the IT department likely have different contact procedures than those inside IT.

5. If the event meets the standard of "Incident," the authority triaging will use determine which specific members of the IRT need to convene and will use the PACE plan to contact them. The IRT will meet physically or virtually via a secure, out of band system, and determine a strategy:

   a) Is this incident real or a false positive?

   b) Is the incident ongoing?

   c) How does this impact our ability to go to market and win?

   d) What is the business impact should the attack succeed? See Incident Categories

   e) What assets are threatened and how critical is an immediate response?

   f) and Categories of Information Impact tables to understand the impact. Contact relevant people that may provide more information to severity.

   g) What systems or systems are targeted, where are they physically or on the network?

   h) Is the incident inside a high-value or supposedly isolated network, infrastructure, SaaS, platform or otherwise elevated system of trust?

   i) Is this a break-glass-in-case-of-fire incident (how urgent is this)?

   j) Can we quickly contain the incident?

   k) Will the response alert the attacker and do we care?

   l) What type of incident is this?

   m) Who else needs to know?

6. The IRT will create an incident ticket and the incident will be categorized into the highest applicable level as established in the policy section of this appendix.

7. The IRT will begin taking time-stamped notes on the ticket itself (technology permitting).

8. Select the appropriate plan or playbook based on the initial assessment of the incident. If an appropriate plan does not exist, create an initial plan.

9. New plans created must be documented so that they can be encapsulated after recovery is complete.

10. Notify any additional personnel as appropriate or indicated by the playbook.

11. All incident response team members begin work to contain the incident and gather additional information.

12. Talk to witnesses (if any) and begin scrubbing logs (and gaps), alerts, and system availability tools to determine root cause and impact. Note: Only authorized personnel appropriate for the situation should perform interviews or examine the evidence. If in doubt consult the CISO and legal counsel.

13. Forensics evidence and data will be gathered and maintained in accordance with the policy section of this appendix.

14. The incident response team will work with other stakeholders (such as the NOC) and will recommend changes to contain and prevent the incident from expanding and recurring.

15. All changes will be annotated in the incident response ticket

16. Management will approve changes, potentially expediting or modifying normal change control processes to appropriately mitigate risks. Any change or departure from normal procedure will be documented in the ticket.

17. If the incident is a system compromise, team members will remediate the incident and restore the affected system(s) to an uncompromised state. They may do one or many of the following:
    a) Re-install and restore data from backups if necessary. Note: Verify if you are required to preserve evidence before executing!
    b) Rotate passwords if there is a reasonable possibility they have been disclosed.
    c) Be sure the system has been hardened by turning off or uninstalling unused services.
    d) Validate appropriate patching levels.
    e) Validate that intrusion detection/EDR/other protections are running.
    f) Validate appropriate logging and reporting.

18. If the incident is a DDoS:
    a) Determine if the Internet provider cut the circuit and why. If they turn the circuit back on and there's still an ongoing DDoS, the circuit may flop again. This would require scrubbing prior to traffic landing on the circuit.
    b) Determine if the DDoS is a noisy feint designed to take your attention away from a more nefarious goal.

19. If the incident is ransomware, follow your ransomware playbook. This may require:
    a) Contacting outside counsel
    b) Implementing your external Communications Plan
    c) Validating backup integrity
    d) Identifying and remediating root cause

20. All the following will be documented:
    a) How the incident was discovered.
    b) The category of the incident.
    c) How the incident occurred, whether through email, firewall, etc.

d) Where the attack came from, such as IP addresses and other related information about the attacker.

e) What the response plan was.

f) What was done in response?

g) Whether the response was effective.

21. After documentation is compiled, notify proper external agencies:
    a) If prosecution of the intruder is possible, notify the police or other appropriate agency
    b) Compile a list of all agencies to contact, contact information, and the date/time they were contacted
22. Assess damage and cost to the organization and estimate both the damage cost and the cost of the containment efforts.
23. Review response and update policies. Plan and take preventative steps to prevent re-compromise or the intrusion from recurring.
24. Consider whether an additional policy could have prevented the intrusion.
25. Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.
26. Was the incident response appropriate? How could it be improved?
27. Was every appropriate party informed in a timely manner?
28. Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?
29. Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
30. Have changes been made to prevent a new and similar infection?
31. Should any security policies be updated?
32. What lessons have been learned from this experience?

4 Appendix C: Asset Management Policy

4.1 Overview and Purpose

1. The purpose of this policy is to ensure that IT and information security support COMPANY and allow it to win in the marketplace by establishing guidelines for managing assets both informational, virtual, and physical.

2. This policy establishes the principles by which COMPANY manages its assets including but not limited to computers, servers, software, information, and other critical assets.

4.2 Scope

This policy applies to entities as outlined in the Cybersecurity and IT Policy base document. Specifically, this document outlines applies to all information assets owned, leased, or otherwise used by COMPANY or which store COMPANY's information. Examples of IT assets include hardware such as user devices including endpoints and/or phones, office assets (cameras, printers, access points), software, various as-a-service assets such as Infrastructure (IaaS) and Software (SaaS) platforms like Google Workspaces, AWS, GitHub, QuickBooks, Salesforce, etc.

4.3 Enforcement

See enforcement clause in the Cybersecurity and IT Policy.

4.4 Roles and Responsibilities

1. The CISO or equivalent person designated in writing is responsible for proper implementation of the Asset Management Policy and accountable for driving the program.

2. The IT Team is responsible for maintaining accurate inventories and tracking systems for all assets and for deploying, operating, and maintaining asset management tools.

3. Directors are responsible for knowing their own inventories and keeping the IT Team and CISO informed of adds and changes

4.5 Acronyms and Terms

Asset management - The process by which our organization will identify, inventory, maintain, and dispose of physical and virtual assets.

4.6 Policy

1. Inventory of Computational Assets.
    a) The IT Team, with the advice and assistance of the information security team, will maintain an accurate inventory of all COMPANY's assets at all times. To the extent possible, COMPANY will record the following information for all computation assets and may adapt this list for physical versus logical assets:
        i. 1. Device name

ii. Device serial number (or equivalent unique identifier for virtual servers)
iii. Device IP addresses
iv. Device MAC addresses
v. Device FQDN
vi. Firmware and/or Operating system Version and date
vii. Date of purchase and/or deployment
viii. Date when the asset will exceed end of life, warranty, or support
ix. Date of when service contracts will expire
x. Date of when COMPANY must give notice by to avoid auto renew if applicable
xi. Date installed
xii. Classification level
xiii. Department or unit
xiv. Physical location
xv. Point of contact
xvi. Brief description of role
xvii. In addition to an inventory, COMPANY will maintain a map, diagram, or other pictural representation of how assets are dispositioned or segregated physically and logically.

2. The Asset Inventory can be found here: LINK_TO_ASSET_INVENTORY
3. The Network Map can be found here: LINk_TO_NETWORK_DIAGRAM

4.7 Inventory of Software and Services

1. The IT Team, with the advice and assistance of the information security team, will maintain an accurate inventory of all of COMPANY's software and services. To the extent possible COMPANY will record the following information for all software, services, or IT related subscriptions:
   a) Vendor name
   b) Internal point of contact
   c) Vendor point of contact
   d) Type of software, service, or subscription
   e) Version number
   f) Account Number (such as for the license or with the vendor)
   g) Quantity
   h) Cost
   i) Billing Period
   j) Expiration or renewal date

k) End of life or support

l) Date of when service contracts will expire

m) Date of when COMPANY must give notice to avoid auto-renewal if applicable

n) Department or unit

o) Description

2. The software and services inventory should include IaaS and SaaS services, software deployed on servers or user workstations, both open-source and proprietary, services hosted by third parties, domain names, and other related registrations or subscriptions.

3. For development processes, the development department leader is responsible for tracking all software dependencies and packages in use throughout the development and production pipeline and environments and reporting those inventories to IT for tracking. This supports the concept of a software bill of materials (SBOM), allowing the team to understand inventory risk.

4. The Software and Services inventory can be found here: LINK_TO_ASSET_INVENTORY

4.8 Inventory of Critical Accounts

1. Critical or privileged accounts, either for users, administrators, or automation, will be tracked and managed with the same scrutiny as other assets and will be considered critical to COMPANY accomplishing its mission and winning in the market.

2. Critical accounts include but are not limited to any key provided to a third party to access COMPANY's systems, root or system level credentials of any kind, AWS root credentials, and the personal credentials of any COMPANY level executive.

3. An inventory of Critical Accounts will record:

a) Name

b) Account name

c) Date provisioned

d) All people with access to that account or credential

e) Privilege level

f) Date of last review or audit

4. The Critical Account inventory can be found here: LINK_TO_ASSET_INVENTORY

4.9 Asset Provisioning (and Gold Image)

1. The IT team will establish "gold images" for all configurable assets COMPANY relies on.

2. COMPANY will establish a gold image for at least each of its servers, baseline container images, and user workstations and will review each gold image when it is changed or updated to ensure that any vulnerabilities or security issues are properly documented and mitigated. Each image will be reviewed at least annually.

3. When a new asset is acquired or deployed, it will be configured using COMPANY's gold images and confirmed before it is deployed to development, staging, or production environments. IT will manage code, scripts, or other automated means to deploy gold images, set initial configurations, and provide updates to the extent possible.

4. COMPANY's gold images are stored and documented here: LINK_TO_GOLD_IMAGE_LIST

4.10 Configuration Management

1. Configuration management drives patch management

2. COMPANY has a vested interest in investing in the care and feeding (lifecycle management) of its assets. Using Gold Images is the correct place to start. Keeping those Gold Images and all their deployed subordinates up to date is nontrivial.

3. Patching is hard.

4. An IT Team with a solid configuration management program manages the Gold Images and deploys configuration updates through that management. This means that patches happen as an outcome of a define-one-deploy-many configuration management program rather than a box-to-box patching program.

4.11 Tools for Asset Control

1. The IT team, with the advice and assistance of the information security team and relevant third parties, will establish tools for monitoring the state and health of assets. Such tools will be deployed to all COMPANY assets which can receive them and will be used to track:

2. What asset is active and where (at least to a logical, network level)

3. What the asset's running state is

4. What accounts, services, or personas are leveraging the asset

5. What software, services, or libraries are present or active on the asset

6. Where possible, asset control tools will also provide end point protection and enable the collection of logs and other artifacts relevant to asset management and incident response.

7. Further documentation regarding COMPANY's asset management tools can be found here: LINK_TO_EDR_OR_RMM_TOOLS_DOCS

5 Appendix D: Acceptable Use Policy

5.1 Overview and Purpose

1. The purpose of this policy is to establish acceptable and unacceptable use of data, information, network resources, and electronic devices at COMPANY in conjunction with a culture of ethical and lawful behavior, openness, trust, and integrity that allow COMPANY to remain competitive in a crowded market.

2. COMPANY provides computer devices, networks, and other electronic information systems and access to information and services to meet COMPANY goals, initiatives, and to serve clients and stakeholders. COMPANY must manage its information systems and assets responsibly to maintain confidentiality, integrity, and availability of its assets and information. Users granted access to COMPANY assets must then serve as stewards of those assets and comply with applicable policies.

5.2 Scope

This policy applies to entities and assets as outlined in the Cybersecurity and IT Policy base document.

5.3 Enforcement

See enforcement clause in the Cybersecurity and IT Policy.

5.4 Roles and Responsibilities

This policy inherits Roles and Responsibility from the Cybersecurity and IT Policy in the base policy document.

5.5 Acronyms and Definitions

1. Honeypot, Honeynet - technical infrastructure that serve as early-warning systems.

2. Spam - Electronic junk mail or junk newsgroup postings. Messages that are unsolicited, unwanted, and irrelevant.

5.6 Policy

1. General Requirements
    a) COMPANY proprietary information stored on devices, whether owned or leased by you, COMPANY, or a third-party, remains the sole property of COMPANY. COMPANY personnel may access, use, or share COMPANY proprietary information only to the extent it is authorized and necessary to fulfill their assigned job duties.
    b) You are responsible for exercising good judgement regarding appropriate use of COMPANY resources in accordance with all COMPANY policies, standards, and guidelines. COMPANY resources shall never be used for any unlawful or prohibited purpose.

c) You shall not take any action that hinders, reduces, or otherwise interferes with COMPANY's ability to go to market and win. You shall not negatively impact the COMPANY's confidentiality, integrity, or availability of and or to assets without proper authorization from the correct authorities at the COMPANY. For questions about which specific people or committees may authorize such an action, see COMPANY's legal department and COMPANY leadership.

d) For security, compliance, and maintenance purposes, COMPANY may authorize personnel or assets to monitor and audit all infrastructure, user accounts, and systems per the IT and Cybersecurity Policy. Often, these include network and endpoint scanning. To achieve a high-degree of success and inventory of current vulnerabilities, approved audit leaders may disconnect or temporarily disable systems, such as various forms of firewalls, that prevent scans. Users may not actively block authorized audits or scans.

2. Accounts, Passwords, and Credentials

a) You are responsible for and the steward of all data, information, user accounts, technical infrastructure, and computers systems under your control and or custodial responsibility.

b) All accounts or the equivalent of an account will be protected by a username, and password, and multifactor authentication when applicable and available. As technology changes and COMPANY implements that same technology this clause may have exceptions.

c) You will protect all accounts or access with strong passwords that meet the following criteria:

   i. Must be 20 or more characters long.

   ii. Must contain at least one capital letters, one numbers, and one special character

d) Passwords will not be stored unencrypted at any time and should be stored within one of the COMPANY's approved password managers provided here:

   i. PasswordManager using an official COMPANY email address

e) In addition to a password, users shall protect accounts or access with an additional factor using a COMPANY approved multi-factor authentication tool. You are allowed to use either of the following tools with a mobile phone and your COMPANY accounts:

   i. Google Authenticator

   ii. Authy

   iii. Azure Authenticator

f) SMS (text messages) are NOT approved for use with COMPANY-associated accounts that have multi-factor authentication as an option. Services that do not offer multi-factor authentication or are forcing SMS should be reported to and tracked by the security team.

g) We recommend using a backup phone, when possible, to save your MFA seeds to reduce impact following a lost or stolen device.

h) User accounts and accesses, including passwords, will not be shared with anyone at any time including the IT team, badged personnel, third party stakeholder, family, or friends. Doing so, regardless of the reason, is a violation of this policy. Exceptions must be documented in the Exceptions register.

i) In some cases, a shared account may be authorized to co-manage services that do not support identity access management or role-based controls. In such cases, the shared account must be approved by the CISO and documented by the IT Team. Credentials for all such shared accounts will be stored in the approved password manager in such a way that the IT Team can enforce and monitor role-based access of the shared credentials.

j) Change default and initial passwords and other credentials as soon as you acquire them. This is non-negotiable.

k) Should an account, access, credential, or password ever be compromised or disclosed, that credential must be immediately changed unless otherwise approved by the security team who is authorized to weigh the costs and benefits associated with the high-risk alternative.

l) You must ensure through legal and or technical means that proprietary information and critical data—especially PII and payment card data—always remain within the COMPANY's control.

m) Conducting COMPANY business that results in the storage of proprietary information on personal or non-COMPANY controlled environments, including devices maintained by a third-party with whom COMPANY does not have a contractual agreement is prohibited. This specifically prohibits the use of an email account that is not provided by COMPANY or its customers and partners for COMPANY business.

3. Computing Assets

a) You are responsible for ensuring the protection of assigned COMPANY assets that includes the use of computer cable locks and other security devices. Laptops and desktops left at COMPANY overnight will be secured by a locked door or with a cable lock at a minimum. When possible, laptops and other portable devices will be stored in a locked drawer or cabinet.

b) Promptly report any theft or loss of COMPANY assets to the Facilities Manager and to the IT team.

c) All PCs, PDAs, laptops, workstations, or computing equipment must be secured with an automatic lockout after 10 minutes or less. You must lock your computer or log off when your device is unattended.

d) Devices that connect to the COMPANY network must comply with the IT and Cybersecurity Policy.

e) Do not interfere with COMPANY's device management or security systems or software, including but not limited to:

i. List of COMPANY tools

ii. Remote Management tools

iii. EDR tools

iv. MDM tools

v. Other tools

f) When traveling with COMPANY devices, devices are NOT to be left unattended. Specifically, you are not allowed to leave COMPANY devices in any vehicle. The highest probability of loss of a device is when YOU leave it in a car while you go to dinner. This is not acceptable.

g) When at home, devices must be kept in a separate location with the ability to limit physical access by other people in the household. A locked bedroom door or desk drawer are acceptable.

4. Asset Use

a) You are responsible for the security and appropriate use of COMPANY network resources under your control. Using any COMPANY resources for the following is strictly prohibited:

i. Disclosing COMPANY intellectual property or controlled information.

ii. Causing a security breach to COMPANY assets which you are not authorized, circumventing user authentication on any device, or capture network traffic.

iii. Causing a disruption of service to either COMPANY or any other network resources including but not limited to ARP cache poisoning, DoS/DDoS, etc.

iv. Accessing COMPANY assets for any purpose other than conducting COMPANY business.

v. Introducing any technology, equipment, or data to the COMPANY network or platforms without approval from the IT Team.

vi. Hosting, copying, or using unlicensed content or software or any content in a way that violates the intellectual property rights of another entity.

vii. Exporting or importing anything that would violate any applicable export control laws.

viii. Use of the internet or COMPANY network that violates the IT and Cybersecurity Policy, COMPANY policies, or local laws.

ix. Intentionally introducing malicious code.

x. Conducting any offensive or defensive cybersecurity actions that you are not specifically authorized to do and only when windows that you are authorized to do them.

b) Termination of Access

i. The IT or Information Security Team will revoke terminated users' access to COMPANY assets and accounts immediately upon the effective date of terminated employment, contract, or agreement regardless of whether the termination was voluntary or involuntary except when legal hold, investigation, or other conditions necessitate. During such exceptions, the user's access will be terminated but the account and data will be maintained unchanged.

ii. Terminated access applies to both individual accounts and any approved, shared accounts.

iii. COMPANY may terminate access for employees in other situations as required.

c) Electronic Communications

i. The following are strictly prohibited:

A. Inappropriate use of any COMPANY asset to conduct any illegal or criminal activity or transmit any communication that violates the Employee Handbook. Examples include disclosing intellectual property, harassing anyone, or breaking laws.

B. Fraud: Making fraudulent offers or forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.

C. Making statements about warranty, expressly or implied, unless it is part of normal business duties assigned.

D. Posting the same or similar non-business-related messages to large numbers of online forums, social media, public messaging groups, newsgroups.

E. Use of a COMPANY email or IP address to engage in conduct that violates COMPANY policies or guidelines. Posting to a public forum, messaging service, social media account, newsgroup, bulletin board, or other messaging board with a COMPANY email or IP address represents COMPANY to the public; therefore, you must exercise good judgement to avoid misrepresenting or exceeding your authority to represent the opinion of COMPANY—any social media post from a COMPANY email address or IP address should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of COMPANY unless posting in the course of business duties.

5. Annual Training

a) All staff and employees must complete annual security trainings and participate in any simulations or exercises conducted by the information security or IT teams.

6. Exceptions

a) Deviations from or exceptions from these policies shall be submitted to the CISO and IT Team for approval and documentation respectively.

7. Agreement

By signing below, you indicate that you have read the above requirements and policies for acceptable use of COMPANY information systems and understand your responsibilities regarding the use of COMPANY systems and assets and the information contained in them.

NAME: _____
DEPARTMENT: _____
SIGNATURE: _____
DATE: _____

6 Appendix E: Change Management and Change Control Policy

6.1 Policy Statement

This policy exists to ensure that we adequately plan for, document, react to, and learn from changes we make to our operating posture.

6.2 Purpose

The purpose of this policy is to ensure that information security increases our ability to win in the market and against our competition.

6.3 Definition

Change Management refers to a formal process for making changes to IT systems. The goal of change management is to increase awareness and understanding of proposed changes across an organization and ensure that all changes are made in a thoughtful way that minimizes negative impact to services and customers.

6.4 Scope

1. This policy applies to entities as outlined in the Cybersecurity and IT Policy base document.
2. All Changes to IT services must follow a structured process to ensure appropriate planning and execution.

6.5 Steps

1. Planning: Plan the change, including the implementation design, schedule, communication plan, test plan, and roll back plan.
2. Evaluation: Evaluate the change, identify the nature of the change and what assets could be impacted, quantify the impact of an outage to those assets, determine risk level, and select the appropriate change type and change process to use.
3. Review: Review change plan with peers and/or Change Advisory Board as appropriate to the change type.
4. Approval: Obtain approval of change by management or other appropriate change authority as determined by change type. Communication: Communicate about changes with the appropriate parties (targeted or organization-wide). For example, any change that could impact users must be communicated well in advance!
5. Testing: Test proposed changes in a realistic environment and prepare for fallback or rollback procedures. Capture lessons learned and build runbooks where appropriate. The perfect example of a change that requires a runbook is for user-impacting changes. Build runbooks for the help desk to use to solve friction during rollout.

6. Implementation: Implement the change while anticipating a need to fallback or revert in the event of an outage. For large system changes and for user-impacting changes, implement a phased rollout. For example, when rolling out multifactor authentication, test rollout with the security team first, and then a subset of privileged users, and then a subset of unprivileged users, and then by department.

7. Documentation: Document the change and any review and approval information. The documentation phase will include capturing feedback from the following:
   a) Departments or persons negatively impacted by the change
   b) The teams responsible for rolling out the change
   c) Stakeholders with significant investment into the change
   d) Any emergency personnel or teams pulled in to aid the rollout
   e) Post-change review: Build the foundation that enables better, faster change in the future.
   f) This phase may be the most important phase of the change process.
   g) This phase is designed to streamline further organizational change.
   h) This phase allows future change agents a platform to better understand the organization and infrastructure which enables them to build a better plan and avoid previous, known pitfalls.

6.6 Authority

Department heads are responsible for the change management process within their department and responsible for coordinating and deconflicting with change outside their department. For measures that require additional funding, the department heads must consult Finance during the Approval step.

6.7 Documentation

1. a. All Normal and Emergency changes, evaluations and approvals will be documented to allow customers to understand what was changed, the reason it was done, and the process that was used to make a change. The following details the kind of information that will be logged for each change and where it will be logged. b. Change Log
   a) All Standard, Normal, and Emergency changes are logged in the Change Log i
   b) The Change Log contains:
      i. Who made the change
      ii. What was changed
      iii. Why the change was made (Reason/Comment)
      iv. And when the change was made
   c) Process Log
      i. Normal Medium, Normal High, and Emergency changes are logged in the Process Log

ii. The Process Log contains
    A. Test Plan and testing results
    B. Risk assessment documentation
    C. Communication Plan
    D. Deployment Plan, including back-out contingencies

7 Appendix F: Remote Working Policy

See Employee Handbook

8 Appendix G: Security Awareness Policy and Program

8.1 Policy Statement

This policy exists to drive stakeholder vigilance against incidents and motivate the team to report both potential and confirmed incidents.

8.2 Purpose

aWe win in the marketplace when we secure ourselves in the marketplace. That security requires us all users to strive to the collective goal of protecting our information and our assets.

8.3 Scope

1. This policy applies to entities as outlined in the Cybersecurity and IT Policy base document.
2. All COMPANY users and external entities with access to COMPANY information or information systems must receive training.

8.4 Policy

1. This policy is to educate users about risks to information and information systems and drive appropriate action at their privilege level. The COMPANY security training and awareness program includes security awareness presentations, security reminders, general security training, system-specific security training, security management training and professional security education for members of the workforce. Additionally, our awareness and education program will include the following:
   a) Annual mandatory training.
   b) Scheduled awareness surveys.
   c) Periodic unscheduled awareness assessments to assure compliance with the training.
   d) Feedback surveys to improve our awareness training and education program.
   e) Phishing campaigns.
   f) Social hacking campaigns.
   g) Live-person physical penetration tests.
   h) Special training for privileged account users and information custodians including but not limited to incident response training, incident response exercises, forensics training, government reporting, and chain of custody.
2. When applicable, training completion and results will be maintained in the individuals Human Resources personnel file, as part of the permanent record.

8.5 Responsibility

The CISO is responsible for this program, its direction, and its effectiveness with input from legal, HR, and the IT Committee.

9 Appendix H: Business Continuity Policy and Plan

To be published

10 Appendix I: Technical Security Policy

10.1 Policy Statement

This policy exists to ensure that we can appropriately design an overall technical security policy that can serve as a focus for our technical security strategy.

10.2 Purpose

The purpose of this policy is to ensure that technical security policy increases our ability to win in the market and against our competition.

10.3 Scope

This policy applies to entities as outlined in the Cybersecurity and IT Policy base document.

10.4 Roles

1. Roles are inherited from the base Cybersecurity and IT Policy document. Additions are by exception.

2. Data Loss Prevention Officer - COMPANY can either implement the DLPO role as an additional duty or align the role independently. The DLPO leads the subset of risk mitigation efforts to support the CISO and reduce risk to the partner ecosystem. The DLPO is charged with identifying various data across the organization and classifying it (Identify), building safeguards into the higher levels of data classification (Protect), implementing alarms to understand when that data has left the organization's control (Detect), builds and leads the response to that data lose (Respond), and rebuild that data from backups and engage with stakeholders outside the organization when appropriate to limit the effects of that data loss (Recover).

3. IT Committee - Coordinate with the CISO and DLPO to provide input to the Technical Security Policies are appropriate. The IT Committee will serve at the Change Control Review Board and has a serious but not deterministic voice in controls applied at 49% of the vote versus the CISO. However, the IT Committee can veto projected per-user spend increase of 101% or greater.

10.5 Policy Overview

1. COMPANY will continuously work to decrease our attack surface and improve our security posture by applying the NIST fundamentals of Identify, Protect, Detect, Respond, and Recover to the attack surface that we cannot decrease.

2. We will review both annually and as required by partners or other events such as but not limited to new legislation or otherwise our security compliance requirements. In the event that we have no formal requirement as outlined by local laws, we will apply minimum baselines as required by clients, customers, partners, suppliers, local laws and regulations, and reasonable prudence.

3. We know and understand that "getting hacked" is not a matter of IF, but WHEN. Therefore, we will ASSUME COMPROMISE. This means that we will take those actions that are expected of us throughout our stakeholder network to ensure that we can, on any given day, answer the questions as follows:
    a) Have we been breached?
    b) Have we contained the breach?
    c) Do we have a duty to notify?
    d) Do we need to bring in an external incident response or legal team?
    e) What did the breachers (attempt to) accomplish?
    f) Did we lose anything?
    g) What actions do we need to take?
    h) What is the impact and scope of the breach?
    i) How long will it take us to recover?
    j) If we ASSUME COMPROMISE, then we must continuously endeavor to IDENTIFY, PROTECT, DETECT, RESPOND, and be prepared to RECOVER.
4. Identify
    a) We will continuously integrate our security team with our IT and logistics and operations teams to understand WHAT nodes (devices, infrastructure, software, instances, VPCs, SAAS, etc) are a part of our attack surface. We will use CIS Controls 1&2 to outline how we conduct inventory of those assets prior to bringing those assets into our attack surface and continue to develop our attack surface mapping following because if we know one thing it is that: "We cannot trust our inventory of assets because availability and adaptability often override confidentiality and integrity."
    b) This means we must continue to place sensors to continuously, passively detect changes to our attack surface and actively scan annually externally unless required additionally by some other factor to understand how our attack surface may have changed without the knowledge or understanding of the security team. Often this is described as "Shadow IT."
5. Protect
    a) Understanding that modern systems often have some form of "Shared Responsibility Model" means that we have less control over some systems such as SAAS than we might with other systems such as internally developed and hosted applications run on COMPANY-owned hardware. However, operating within that understanding is not an excuse to assume risk.
    b) While we are strategically a SAAS-focused COMPANY, we will not assume that full responsibility aligns with the provider and we will apply reasonably prudent controls to protect our data and our people. We will apply such controls as multi-factor authentication, security review, vendor risk management programs, and best practices for password policies to limit risk exposure to data in transit, in process, and at rest.

c) User endpoints will be hardened with preconfigured "gold images," will be enrolled in COMPANY-controlled management programs (programs that balance security with personal privacy with preference focused on reasonable privacy), protected with multifactor authentication such as biometrics or other widely accepted factors, protected with increased defenses such as corporate-grade signature and behavioral analytics systems that block suspicious activity, allow-lists when possible, sandboxed email, and other zero-trust fundamentals such as restricted access.

6. Detect

a) Given that we are a SAAS-based, remote-focused COMPANY, our detection measures focus on endpoint, network, identity, and SAAS applications.

b) Identity - COMPANY will implement a zero-trust model of security that focuses on Identity. That means that many of our detection efforts are focused on identity. Therefore, a large portion of our efforts are focused at the identity layer and we will continue to extend our identity integration into SAAS partners such as SalesForce, M365, and other supporting applications as required. This provides us visibility into identity areas that we might not have otherwise understood. This way we can understand where our data is, what our risk exposure is, what adversaries might be attempting to or actually accessing data from compromised identities, and what actions we need to take at the identity layer to limit exposure. Identity logs are pushed to the data aggregation solution to allow for both post-mortems, correlation, and hunt activities.

c) Host (endpoint) - Given that we are a remote workforce, user endpoints are one of our weakest avenues. We can never truly understand whom has access to those devices that might have COMPANY data on them. That means that any user that attempts to access COMPANY data must register the device with COMPANY management before accessing that data. This allows us to detect device health prior and therefore limit access to data for unhealthy devices. This is part of our MDM/UEM strategy. For runtime environments and/or daily operations on those devices, we deploy detection systems appropriate to the hardware and operating system that the user needs. Those detection systems such as host-based intrusion detection systems (HIDS) are often integrated into the same agents running some of the outcomes listed in the Prevent section above. Alerts can be pushed from those endpoints to admins and response teams. Endpoint logs are pushed to the data aggregation solution to allow for both post-mortems, correlation, and hunt activities. This is often done through Intune and the O365 Security Center.

d) Network - For those instances when we do have an office, that office will have an employee and guest network. We will maintain appliances on that network and any remote access solution such as VPN to understand which devices are sending what data to whom. Logs from those appliances (both sensors, and network and security devices) are then pushed to the data aggregation solution to allow for both post-mortems, correlation, and hunt activities.

e) SAAS - While not all SAAS platforms have SAAS logs, we will ingest those logs that are appropriate into our data aggregation solution to allow for both post-mortems, correlation, and hunt activities.

f) Log Aggregation Policy

i. Until we have a compliance framework that requires longer storage, we will store the logs that our aggregation appliance has ingested for 13 months. This number of 13 months is usually more than most regulations require but we've seen multiple times adversaries that are patient enough to wait 366 days to execute their actions because they know most companies shred logs at 365 days.

ii. Whenever possible we will "pre-compute" logs on the node before transmission to limit data volume and velocity into the aggregation solution.

iii. Aggregation solutions need to not only have the capacity to support the incident questions outlined above such as, "Were we breached," but also allow for correlation and hunt activity to help understand where data resides, where it moves, and what is happening to it.

iv. The timeframe here is used as a guiding principle and there may be exceptions under this non-exhaustive list: certain jurisdictions, compliance frameworks, and client contracts.

v. Respond - See Incident Management Policy and Process

vi. Recover - See Business Continuity Policy and Plan

11 Appendix J: Reputation Management

To be published

12 Appendix K: System Lifecycle Management Policy

To be published