Cybersecurity and IT Policy

Ericius Security

01 March 2022

1 Policy Statement

Cybersecurity and IT Policy

1. Policy Statement
   a) TEMP 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.

2. Purpose
   a) The purpose of this policy is to establish cybersecurity guidelines that ensure our ability to accomplish our mission: TEMP MISSION STATEMENT.
   b) 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.
   c) 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.

3. Scope

    a) This policy applies to TEMP 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.

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

4. Enforcement and Expectation of Compliance

    a) 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.

5. Roles and responsibilities

    a) You - As a TEMP 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 TEMP 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.

    b) 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 TEMP COMPANY, which the cybersecurity program and policies support.

c) 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 TEMP 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.

d) Legal Counsel - TEMP 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 TEMP 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.

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

f) IT Team - Execute change in harmony with other stakeholders identified here to maintain the technical ability to execute TEMP COMPANYoperations. Support the needs of TEMP 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 TEMP

COMPANY's assets and infrastructure.

g) 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.

h) Privileged Users - Users of TEMP COMPANYIT and computing assets with administrative or increased access and permissions. TEMP 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.

i) Third-Party Stakeholders - People or entities outside the organization that require access to TEMP 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.

j) 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.

6. Terms

a) 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

TEMP COMPANY. In some contexts, this could include personal devices that have access to TEMP COMPANYassets.

7. Policies

   a) TEMP 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.

   b) TEMP 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.

   c) We will employ countermeasures that include but are not limited to:

      i. Setting program standards

      ii. Risk identification and classification

      iii. Security training

      iv. Identity management and identity-focused security

      v. Change control

      vi. Judicious use of the principle of least privilege (applied zero trust)

      vii. A focus on SaaS-based applications

      viii. Deliberate management of third-party risk

      ix. Securing communications, data, information, infrastructure, systems, endpoints, and owned, leased, or open-sourced platforms.

      x. Out-of-band communications

    xi. Information classification, retention, and disposal

    xii. External audit, assessment, and testing when and where applicable (usually annually)

    xiii. Asset, Vulnerability, and Patch Management

    xiv. Incident Response and Incident Management

    xv. Log and Event Management and Retention

    xvi. Our strategy is simple. As Dustin Wilcox says: "Minimize the Attack Surface, Complicate Unauthorized Access, Rapidly Detect, Respond to, and Contain Incidents."

8. Exceptions

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

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

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

9. Documentation and Control

    a) Documents

        i. This Cybersecurity and IT policy document, all policies or documents contained or referenced herein, and all TEMP 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.

        ii. 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.

    iii. This policy does not apply to log retention, which is governed by a separate policy.

b) Records

    i. 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.

    ii. 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.

c) Distribution and Maintenance

    i. 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.

    ii. The CISO and IT Team maintain a repository of approved policies, both current and historical here: LINK_TO_DOCS_AND_POLICY

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