Cybersecurity and IT Policy

Ericius Security

01 March 2022

Contents

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 orga-

nization 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 pro-

gram 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

2 Appendix A

1. OVERVIEW AND PURPOSE
    a) TEMP COMPANYshall 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 TEMP 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 TEMP COMPANYteam identifies information to support routine disclosure and active dissemination of information, which also helps protect TEMP COMPANY's intellectual property.
    b) This allows TEMP COMPANYto maintain continuous business objectives properly steward information on behalf of relevant parties.
    c) Information is considered a primary asset for TEMP COMPANY. TEMP COMPANYuses multiple types of information assets, and the sensitivity and handling requirements of these information assets may vary.

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

3. Enforcement: See enforcement clause in the Cybersecurity and IT Policy.

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 respon-

sibility for implementing the policy within their respective departments.

5. Acronyms
    a) None for this policy
6. Policy
    a) 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.
7. Classification Categories
    a) TEMP COMPANYcategorizes information into three classes: Public, Internal, and Confidential.
        i. Public - Definition: Information or assets intended for disclosure to or interaction with the public or that, if disclosed, pose no risk or damage to TEMP COMPANY.
            A. Public information includes information assets that do not have any confidentiality or regulatory requirements, or that can be disseminated to the public.
            B. Examples include press releases, annual financial reports in accordance with compliance, marketing material, social media, and TEMP COMPANY's website.
        ii. Internal - Definition: Information or assets that are not intended for public release but do not necessarily pose a significant risk or damage to TEMP COMPANYif released.
            A. Internal information includes information necessary for the organization and operation of TEMP COMPANYthat is not necessarily confidential or information that can be circulated freely within all offices or departments in TEMP COMPANYbut not necessarily the public.

B. Examples include personnel assignments, office orders, internal circulars, movement of personnel or equipment, or invoices.

iii. 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 TEMP COMPANYif improperly disclosed.

A. Confidential information includes information necessary for the business operations of departments or units, information that cannot be freely circulated within TEMP 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.

B. Examples include any information that would reduce TEMP 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.

iv. 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.

8. Secure handling of information assets

a) 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.

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

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

d) Store hard copy confidential information behind double lock and key.

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

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

g) Limit access control both by role and by person/entity.

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

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

j) Limit distribution to "need to know" and "need to use."

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

l) 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.

m) See associated charts, process documents, and controls more granularly here: LINK_TO_INFO_INVENTORY

9. Classification by aggregation

    a) 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 TEMP COMPANY's internal workings that could cause the TEMP COMPANYto lose in a competitive market.

    b) 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.

    c) 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.