ISO 27001:2022 Information Security Management System (ISMS)

**Approval**

The signatures below certify that this ISMS policy has been authorized and demonstrates that the signatories are aware of all the requirements contained herein and are committed to ensuring their provision.

|  | **Name** | **Signature** | **Position/Title** | **Date** |
| --- | --- | --- | --- | --- |
| **Prepared by:** |  |  |  |  |
| **Reviewed by:** |  |  |  |  |
| **Approved by:** |  |  |  |  |

**Amendment Record:**

This ISMS policy is reviewed to ensure its continuing relevance to the systems and process that it describes and a record of contextual additions or omissions is given below:

| **Page No.** | **Context** | **Revision** | **Date** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Purpose

The purpose of this policy is to establish an Information Security Management System (ISMS) at {company} . {company} has established an Information Security Management System (“ISMS”) in accordance with ISO/IEC 27001 (“ISO 27001”) that governs the processes required to protect company and information assets. This document specifies the scope of the ISMS and PIMS at {company} .

# Policy Scope

The policy applies to all company software and hardware infrastructure, devices, systems, and data, covers all company products and services, and must be adhered to by all employees and contractors.

# Ownership

[POLICY OWNER] is responsible for implementing and maintaining this policy.

# Policy Objective

The objective of {company} Executive Management is to continually strengthen and improve the overall capabilities of the ISMS, to increase professional skills in terms of information security management and technology, to make the {company} management system so complete that reliable certification standards are effective, to ensure information- related business operations continue to be carried out to meet certification standards and to establish a sustainable operation plan for business that is cost effective, and to establish quantified information security goals through annual management and review meetings. The objective highlights the following:

* Information is only accessible to authorized persons.
* Confidentiality of information is maintained.
* Integrity of information is maintained throughout the process.
* Business continuity plans are established, maintained, and tested.
* All personnel are trained on information security and are informed that compliance with the policy is mandatory.
* All breaches of information security and suspected weaknesses are reported and investigated.
* Procedures exist to support the policy, including virus control measures, passwords, and continuity plans.
* Business requirements for availability of information and systems will be met.
* The {company} is responsible for maintaining the policy and providing support and advice during its implementation.
* All [company’s managers] are directly responsible for implementing the policy and ensuring staff compliance in their respective departments.

# Scope of the ISMS

The scope of the ISO 27001 certification is limited to the Information Security Management System (ISMS) supporting the assets, technologies and processes employed by {company} located/housed at [location’s name] for [type of services /support] services to its customers.

The scope of information includes the protection of the confidentiality, integrity and availability of information.

The framework for managing information security in this policy applies to all employees within {company}, workers, and other involved persons and all involved systems as defined in Information Security Policy.

This policy and all standards apply to all protected health information and other classes of protected information in any form as defined below in Data Classification.

## **Assets**

The assets of the ISMS are further categorized as information, application, database, cloud services, and personnel:

* [company systems]

## **Locations**

* [company locations]

## **Departments**

The following departments are in-scope for the ISMS:

* [company departments]

## **Personnel**

All personnel belonging to the above departments are in-scope for the ISMS.

### Scope Exclusions and Boundaries

* {company} uses Amazon Web Services (“AWS”) for cloud computing and storage services. Amazon is responsible for managing logical access to the underlying network, system management, and storage devices for its cloud service hosting {company} data.
* Amazon is responsible for the physical security and environmental controls at data center facilities hosting {company} systems; therefore, physical security and environmental controls are out of scope for those facilities.
* Amazon is responsible for the secure deletion of data and disposal of equipment used to support {company} customer operations.
* {company} information, application, database, facility, and personnel assets that are not related to the identified in-scope components are out of scope for the ISMS.

# Information Security objectives

Information security objectives are set and monitored annually by {company}’s ISMS {Committee or Council} based upon a clear understanding of business requirements. The current information security objectives are as follows:

* Protect the confidentiality, availability, and integrity of company, customer, and employee data
* Comply with applicable laws, regulations, and customer contractual obligations
* Achieve and maintain ISO 27001 and [ISO 27701] certifications
* Others

The Action plans to achieve these objectives are maintained and reviewed annually by the ISMS {committee or council}.

| **Objective Description** | **Action Plan to Achieve Objectives** | **Effectiveness Measure(s)** | **Resources Required** | **Owner** | **ETA** |
| --- | --- | --- | --- | --- | --- |
| Protect the confidentiality of customer data | *(i.e Adhere to access control requirements; perform risk assessment)* | *(i.e Remediation plans for high-risk vulnerabilities, etc…)* | *(i.e competent team, etc..)* | *(i.e IS owner)* | *(i.e Ongoing; xx/xx/xx)* |
| Comply with applicable laws / regulations and customer contractual obligations | *(i.e Identify applicable laws / regulations and customer contractual obligations, etc..)* | *(i.e Less than one (1) reportable breach events**, etc..)* | *(i.e competent team, etc..)* | *(i.e IS owner)* | *(i.e Ongoing; xx/xx/xx)* |
| Achieve and maintain ISO 27001 and [ISO 27701] certifications | *(i.e an ISMS, etc..)* | *(i.e Obtaining ISO 27001 certification, etc..)* | *(i.e competent team, etc..)* | *(i.e IS owner)* | *(i.e Ongoing; xx/xx/xx)* |
| Others |  |  |  |  |  |

# Leadership and Commitment

{company} is dedicated to establishing, implementing, maintaining, and continually improving the ISMS. Leadership commitment is demonstrated by the ISMS {committee or council}l when carrying out their responsibilities as defined in section *ISMS* *Roles, Responsibilities, and Authorities*.

# ISMS Roles, Responsibilities and Authorities

Involvement from top management is a critical component to the design and effectiveness of {company}'s ISMS. Specifically, {company} has defined the following management roles and responsibilities:

* The Board of Directors is responsible for oversight of internal controls.
* The ISMS {Committee or Council} is chaired by [Title] and comprises [titles, title]. The council is in place to support information security or drive the future vision of information security.
* Senior management is responsible for making strategic decisions within the organization, and ensuring that the organization's business strategy is aligned with its strategic objectives.
* Managers are responsible for effective management of resources towards accomplishing the security goals.
* Employees are responsible for implementing good security practices.

In addition, {company} ensures that the personnel responsible for its ISMS implementation are competent and knowledgeable.

Personnel’s roles are defined through individual job descriptions in which a {company} manager coordinates directly with Human Resources to develop.

# Interested Parties of the ISMS

{company} defines an interested party as someone, a group or an entity with an interest in the ISMS. These can include staff, suppliers, customers, data subjects, shareholders, directors, prospects, board members, competitors, legislators and regulators, unions, media etc. Other stakeholders might include hackers and related malicious parties with interests in leveraging weakness in the ISMS program.

These interested parties' needs will be considered in more detail as part of the risk assessment process.

| Stakeholders | Impact | Needs /expectation  | Legal obligationsy/n? | Actions Required |
| --- | --- | --- | --- | --- |
| *Staff* | *Medium* | *Clear instructions on security, handling of data.*  | *Yes* | *Training program; Available Policies* |
| *Customers* | *Medium* | *Available service; Data is secured* | *Yes* | *Master Services Agreement Monitoring; Monitoring on Secure practices* |
| *Vendors* | *Medium* | *Achievable contractual agreements* | *Yes* | *Master Services Agreement Monitoring; Monitoring on Secure practices* |
| *Investors* | *High* | *Expect confidence with the organization ISMS program*  | *Yes* | *Monitoring on Secure practices, Third-party Assessment Audits* |
| *Prospects customers* | *Medium* | *Expects assurance of the state of the organization's data security.* | *No* | *Monitoring on Secure practices,Third-party Assessment Audits* |
| *Senior Management* | *High* | *Expect that industry best practices certifications are maintained to provide assurance to the board.* | *No* | *Monitoring on Secure practices,Third-party Assessment Audits* |
| *Board Members* | *High* | *Expect confidence with the organization ISMS program and continual monitoring* | *No* | *Monitoring on Secure practices,Third-party Assessment Audits* |
| *Regulators* | *High* | *Proportionate level of security controls at all times to protect assets. Notification on potential breaches* | *Yes* | *Third-party Assessment Audits, continual Improvement* |
| *Media* | *High* | *Transparency regarding security incidents* | *No* | *System status page, Security Incident Response plan* |
| *Hackers* | *High* | *Interested in weak security practices* | *No* | *Penetration testing, vulnerability scanning,Third-party Assessment Audits* |

# Internal and External Issues

There are a number of internal and external issues that are relevant to the purpose of {company} and that affects the ability of the ISMS to achieve its intended outcome(s).

## Internal issues

With regard to the {company} business itself, there are a number of relevant internal issues.

These include:

* Uncertainties in employee relations
* Significant organizational changes
* Location moves
* Company financial performance
* Company culture
* Resources and knowledge of the organization
* Governance and organizational structure
* Adopted standards and models
* Contractual relationships
* others

These general internal issues will be considered in more detail as part of the risk assessment process.

## External issues

With regard to the external environment in which {company} operates, there are a number of relevant external issues.

These include:

* Political
* Government policy changes
* Government instability
* Unrest in countries in which the organization operates
* Trade restrictions and tariffs
* Economic
* Prevailing economic climate
* Interest and inflation rates
* Supplier failure
* Lack of customer demand
* Increasing globalization of supply and/or demand
* Increasing competition
* Social
* Changing demographics
* Population growth changes
* Social attitudes
* Technology
* Pace of innovation
* Supporting technologies and infrastructure
* Automation and artificial intelligence
* Legal
* Potential legislative changes
* Regulatory changes
* Data protection
* Environmental
* Climate change
* Fire, flood, earthquake etc.
* Pollution
* Others

These general external issues will be considered in more detail as part of the risk assessment process.

# Relevant Laws, Regulations, and Contractual Requirements

{company} identifies, updates, and maintains a current list of all applicable laws and regulatory authorities including relevant contacts to keep up to date with legislations that may affect the achievement of business objectives.

| **Regulation/Authorities** | **Contractual Requirement** | **Circumstances** | **Contact** |
| --- | --- | --- | --- |
| Health Insurance Portability and Accountability Act (HIPAA) | *Office of Civil Rights (OCR) right to audits**Security Rule* | *Breach Notification* | *(202) 690-6343 OCRMedia@hhs.gov* |
| General data Protection Regulation (GDPR) | *Data Protection* | *Data violation* | [*Local DPA*](https://edpb.europa.eu/about-edpb/about-edpb/members_en) *authority:* |
| Professional Associations:International Profession Association (ISACA) | *Maintain yearly CPE* | *Certification upkeep* | *1.847.660.5505* |

# Risk Assessment and Risk Treatment

{company} has defined a Risk Assessment and Risk Treatment Process for identifying, analyzing, treating, and monitoring risks over time. The risk acceptance criteria and analysis has been further documented within the risk register and the risk management policy.

## Statement of Applicability (SOA)

The Statement of Applicability (SOA) defines the information security control objectives and controls as defined by Management based on {company}*,* business needs and requirements considering all relevant legal and regulatory requirements and contractual obligations.

The SOA will be reviewed and approved by management {company},as per the management review procedure.

## Performing Risk Assessments

A Risk Assessment will be performed at least quarterly or may be carried out under the following circumstances with varying scopes as determined by the {Title}. Additionally, risks may be assessed at various levels of the organization for circumstances that include:

* As part of projects that involve significant change to the organization, the ISMS, or the organization’s assets
* Software development and changes
* When third-party suppliers are engaged, changed, or periodically during the relationship
* On major external change affecting the organization which may invalidate the conclusions from previous Risk Assessments, e.g., changes to relevant legislation
* others

Risk Assessments may be carried out as a result of other circumstances at the discretion of the {Title} or ISMS {committee or council}.

## Management Approval

The ISMS {Committee or Council} will be presented with the Statement of Applicability (“SoA”) and highlights from the risk assessment as determined by the {Title}. The entire SoA and risk assessment report shall be made available to the ISMS {Committee or Council} members upon request.

ISMS {Committee or Council} may provide feedback on the risk management process to management during the annual management review or as needed at the discretion of the ISMS {Committee or Council} .

Unless explicit input is received from the ISMS {Committee or Council} regarding the SoA or Risk Assessment, the SoA and all risk treatment plans shall be considered acceptable and approved by the ISMS {Committee or Council} following the Management Review.

# Resources and Competence

Annually, {company} will assess the performance and competence of the personnel against the ISMS required competencies. This will be completed by defining personnel’s role, assessing job performance, and competence during performance reviews and by addressing any competency gaps.

## Measure

Personnel are measured initially for their competence to meet the requirements of the job description throughout the interview process which is inclusive of Human Resources and a {company} Manager. Annually, {company} conducts an employee performance appraisal to evaluate an employee’s performance which is performed by Human Resources and direct managers.

As part of the annual Information Security Awareness training the Information Security Team may issue tests to evaluate an individual’s knowledge and awareness of security topics and company policies.

## Competency Gaps

Solutions for remediating competency gaps will be monitored and evaluated for effectiveness by an individual’s direct manager and documented with Human Resources through the annual employee performance appraisal. Solutions may include providing training or mentoring, re-assigning tasks or personnel, or supplementing with contractors and/or consultants.

Employees who do not pass the security awareness test(s) may be required to complete the training again and retake the test(s), or other remediation activities as needed.

# Training and Awareness

All workforce members are required to complete Security Awareness Training shortly after they join the company and annually thereafter. In addition, they may be asked to complete further training as dictated by operational or environmental changes.

Changes that might lead to adjustment of the training program include:

* A security incident retrospective determining that additional training is required
* Adoption of new technology by the company
* Material changes in organizational policies

A record of the successful completion of each training session must be recorded for each employee. The record may be automatically collected by the training system, or manually gathered by the trainer. Records are retained for a period dictated by compliance and legal requirements.

{owner} is responsible for creating the training program, and for selecting and updating training material over time. The program may be delivered internally, by qualified personnel, or by a third-party vendor.

In addition to the security awareness training, a training program is in place to ensure that employees are up to date with new developments and enhance their skills.

# ISMS Communication

{company} ensures that information security is "front of mind" to all employees, and is not considered a "side issue". Internal communication relevant to the ISMS, such as ISMS updates, security updates, internal audit results including non-conformance remediation activities, and continual effort updates are shared internally with the Board of Directors and senior management as part of internal controls oversight meetings. This information is also shared with all employees as part of company "all-hands" and team update meetings.

In addition, external communications relevant to the state of the ISMS and {company} 's continual efforts to maintain and comply with it are shared on the company's website. External communication will also be on an on-demand basis with customers, prospects, regulators, government agencies (if applicable), and approved third parties.

The communication plan defines the internal publication, scope and operations to be performed:

| **Content** | **Internal / External** | **Recipient(s)** | **Owner /Sender** | **Frequency** | **Method(s)** | **Approval Required** |
| --- | --- | --- | --- | --- | --- | --- |
| ISMS & InfoSec Policies | *Internal* | *(i.e.Employees, contractors, etc..)* | *[title, i.e IS leader)]* | *(i.e, Annually and as needed)*  | *(i.e. intraset, live presentation, etc..)*  | *None* |
| Incident Reports | *Internal* | *(i.e. Security Team**, senior management, etc..)*  | *[title]* | *(according to security incident policy, ie.e within three (3) days of incident resolution)* | *(i.e Reports, security team meetings, etc..)* | *None* |
| Confidentiality agreements | *External* | *Contractors* | *[title, i.e IS leader)]* | *(i.e as needed)*  | *(i.e Email, HR tool,etc..)* | *(i.e Legal, HR, ETC..)* |
| Other |  |  |  |  |  |  |

# ISMS Documentation

{company} has identified a set of mandatory documented information relating to its ISMS, and has established a process to share, communicate, update, and retain this documentation. All documented information pertaining to the ISMS is maintained in the company's compliance management tool, as well as in internally-shared storage.

“ISMS Documents” shall include both ISMS Management Policies as well as Information Security Policies.

| **Document Name** | **Storage Location** | **Ownership** |
| --- | --- | --- |
| ISMS policy | (i.e Trust Cloud and internal drive) | ISMS Council or committee |
| Access Control Policy | (i.e Trust Cloud and internal drive) | IS Team |
| Asset Management Policy | (i.e Trust Cloud and internal drive) | IS Team |
| Business Continuity and Disaster Recovery Plan | (i.e Trust Cloud and internal drive) | IS Team |
| Cryptography Policy | (i.e Trust Cloud and internal drive) | IS Team |
| Data Management Policy | (i.e Trust Cloud and internal drive) | IS Team |
| Human Resource Security Policy | (i.e Trust Cloud and internal drive) | IS Team |
| Incident Response Plan | (i.e Trust Cloud and internal drive) | IS Team |
| Information Security Policy | (i.e Trust Cloud and internal drive) | IS Team |
| Operations Security Policy | (i.e Trust Cloud and internal drive) | IS Team |
| Physical Security Policy | (i.e Trust Cloud and internal drive) | IS Team |
| Risk Management Policy | (i.e Trust Cloud and internal drive) | IS Team |
| Change Management Policy | (i.e Trust Cloud and internal drive) | IS Team |
| Vendor Management Policy | (i.e Trust Cloud and internal drive) | IS Team |

##  Document Format

The format of all documents will be electronic. If hard copies are required, personnel are encouraged to print directly from the source repository to ensure current versions are used. Any printed or locally saved documents are uncontrolled.

Each document consists of a document name, purpose and approval records.

## Document Approvals

The documentation is updated and approved annually, and the most recent version is made available to all employees. A historical approval log is used to track any changes made to the documentation.

## Documentation Archival, Retention, and Disposal

The ISMS {Committee or Council} is the final authority, which approves the ISMS Documents. The Information Security Management Leader is responsible for implementing ISMS {Committee or Council} directive and maintaining and approving changes to policies and procedures (including communicating the latest version of the document).

All documentation is retained for a period of at least six years after its creation. Approved documents exceeding their useful life are stored in an archive order to form an audit trail of document development.

Archived documents will be maintained for at least three (3) years. Once it has been decided to dispose of ISMS Documents, they shall be deleted in a secure manner consistent with company policy.

# ISMS Internal Audit (IA)

The purpose of this policy is to define the objectives, authority, and responsibilities of the Internal Audit role within {company} . The mission of Internal Audit is to assist company management in effectively carrying out their responsibilities, by providing management with evaluations on the effectiveness of internal compliance and governance processes, and making recommendations for improvements.

The internal audit is used to help determine whether the ISMS control objectives, controls, and policies and procedures:

* Conform to the applicable requirements of the ISO/IEC 27001 (“ISO 27001”) standard
* Conform to the identified information security requirements
* Are effectively implemented, maintained, or have opportunities for improvement

## Scope

The audits will cover all elements of the ISMS for all in-scope information assets and the applicable controls identified within the Statement of Applicability.

## Auditor Selection

The Information Security Team may engage a third-party vendor knowledgeable in performing ISO 27001 internal audits. The auditor(s) should be trained and/or otherwise qualified to perform the internal audit of an ISMS. It should also be confirmed that there is proper segregation of duties while choosing an auditor (i.e., the auditor has not implemented or does not operate or review any of the controls under audit).

The auditor(s) shall be evaluated based on their education and experience to validate their competence.

## Resources

The third-party internal auditor(s) will carry out the audit program with input from the Information Security Management Leader and the Information Security Team.

The primary responsibilities of the internal auditor are as follows:

* To plan the ISMS internal audit(s) as per the defined frequency and schedule
* To conduct the internal audit as per the audit plan and to share the results of the audit findings with the Information Security Leader for review and approval
* To ensure the confidentiality and integrity of the audit data and the supporting evidence within the auditor’s control
* To provide all audit records to the Information Security Leader as requested
* To identify the corrective actions to be taken to close the audit observations/non-conformities, to review the actions taken to close the gaps reported, and to evaluate the effectiveness of such actions

## Frequency & Schedule

The frequency of the internal audit is scheduled to be conducted annually at minimum. The ISMS {Committee or Council}will determine if the frequency of the audit needs to be increased depending upon the number of findings identified during the audit, the severity of the previous audit findings, and the operating efficiency of conducting the audit annually.

## Audit Criteria

The audit criteria shall take into consideration the defined set of ISMS policies and procedures, any regulatory, legal, and contractual requirements, ISO 27001, and any additional authoritative standards as necessary.

## Evaluation Criteria and Alternative Labeling of Findings

A non-conformity (“NC”) is a gap against the ISO 2700 standard which may have an adverse effect on the interests of ISMS.

* ***Major NC*** - the adverse effect is immediate and directly impacts the ISMS’ ability to achieve its objectives
* ***Minor NC*** - the effect may take place over a period of time and does not immediately adversely impact the ISMS
* ***Conforms*** - controls are designed and operating effectively in accordance with the requirements of ISO 27001
* ***Opportunity for Improvement (“OFI”)*** - an observation may arise out of an opportunity for improvement

{company} reserves the right to apply any appropriate internal audit of information security controls to the ISO 27001 internal audit requirements.

 Alternative audit approaches may identify findings using alternate terms such as “Yes/No/Partial,” or “In Place/Not in Place.” In cases where an alternate standard or approach is applied to the ISO 27001 internal audit requirements, the controls will be “mapped” to ISO 27001 Controls and the finding language will be mapped to ISO 27001 evaluation criteria. For example, controls labeled, “Yes,” and, “In Place,” may be mapped to ISO 27001 as, “Conforms.”

## Audit Documentation

The internal auditor shall audit the ISMS policies and procedures, implement information security controls, and the effectiveness of the ISMS against the ISO 27001 standard requirements. Artifacts and documents may be collected as evidence by the auditor in addition to observations and interviews.

## Audit Reporting

The internal auditor shall document the audit results and observations along with the supporting evidence. A final report will be produced and shared with the Information Security Leader for initial review and finalization. Highlights of the internal will be communicated to the ISMS {Committee or Council}. The complete internal audit report will be provided to the ISMS {Committee or Council} upon request. An internal audit report will show the audit results including non-conformities and observations.

## Audit Records Retention

The evidence collected and the documentation prepared as part of the internal audit shall be protected and retained in accordance with the requirements defined within the *ISMS Documentation* section.

# Management Review

{company} has defined an ISMS Management Review Procedure consisting of the necessary inputs and outputs to ensure that the company’s ISMS is operating effectively, as intended, and is continually improving. The management reviews may include the following inputs as determined by the {owner}:

* Changes in the internal or external context of the organization
* Changes in needs and expectations of interested parties
* Feedback from interested parties
* Changes in leading practice and guidance
* Changes in legal, regulatory, or contractual requirements
* Risk acceptance criteria
* Results of the risk assessment
* Status of the risk treatment plan and implementation plan
* Effectiveness monitoring and measurement results
* Internal audit results
* Status of action items from previous management reviews
* External third-party audit observations (e.g., external certification audit)
* Status of open non-conformities, corrective actions, and improvement plans
* Trends in non-conformities and corrective actions
* The results of the training program used to assess the level of information security awareness within the organization
* High risk incidents and the related root cause analysis and action plans
* Trends in internal information security incidents
* Results of any penetration or other technical tests
* Results from any privacy-related inquiries and the company response
* Information Security performance and the effectiveness of the information security management system
* Any information security contacts, inquiries, warnings or penalties from a governmental or regulatory body
* Other items at the discretion of the Information Security Leader or the ISMS Governance Council
* Status of and/or results from any information security-related audit (i.e., certification, customer, etc.)

The ISMS {Committee or Council} shall review the summary of the review inputs, the analysis of the inputs, and the proposed key decisions and actions. The ISMS {Committee or Council} will approve the review, results, and any final decisions/ actions needed. These decisions and actions may include the following:

* Changes to the ISMS scope and boundaries
* Action items to improve the effectiveness of the ISMS
* Modifications to the information security policies, objectives, and related procedures
* Updates to the risk assessment, risk treatment plan, and implementation plan
* Identification or modification of resource and/or funding requirements needed to improve the ISMS or to execute defined plans (e.g., implementation plan, correct action plan, etc.)

The ISMS {Committee or Council} shall review the effectiveness measures for ISMS controls:

* The ISMS {Committee or Council} is responsible for reviewing the control effectiveness measures at least annually.
* The Information Security Team will prepare the meeting presentation for the ISMS {Committee or Council} by outlining the Measurement & Metrics and adding them to the presentation.
* The Information Security Team will identify if the current metric exceeds the levels defined in the Measurement & Metrics criteria.
* If a metric exceeds its Criteria, then the ISMS {Committee or Council} will discuss actions which must be taken to correct the deficiency which allowed the control to become ineffective. Actions will be recorded in the Corrective and Preventive Action Plan.

# Corrective Action and Continual Improvement

{company} has defined an ISMS Corrective Action and Continual Improvement Procedure when non-conformities are identified. Non-conformities may be identified during internal audits, external audits, management reviews, or ongoing monitoring of the ISMS.

## Criteria

The following criteria may result in the identification of corrective actions and improvement opportunities which will be used to help drive the continual improvement:

* Non-conformities (“NC”) (major and minor) or observations identified during third-party audits (e.g., certification audits)
* Opportunities for Improvement (“OFI”) or observations identified during internal audits

## Corrective Action Plan Requirements

The corrective action and improvement plan items shall be added to the Risk Register and Treatment Plan and shall contain the following information at a minimum:

* Risk description or vulnerability
* Risk treatment plan or corrective action
* Risk or implementation owner
* Remediation ticket reference number(s) (if relevant)

The Information Security Team shall validate that the following supporting documentation is updated, if needed, based on the results of the completed corrective action (or improvement):

* Internal and external factors within the ISMS scope and boundaries
* Controls, policies, and procedures
* Risk Assessment and Risk Treatment Plan
* Effectiveness measure of the control.

## Monitoring

On an annual basis, the ISMS {Committee or Council} shall monitor the status of any open items on the corrective action and improvement plan and discuss actions needed to complete these items.

# Policy Violation

All {company} personnel (including employees, contractors, and applicable third parties) must maintain the security, confidentiality, availability, integrity, and privacy of {company} assets. Violations of ISMS policies and procedures may be considered serious breaches of trust, which can result in disciplinary action up to and including termination of employment or contract and prosecution in accordance with applicable federal, state, and local laws.