**COMPANY Logo**

**Information Security Policies:** Information Security Management

Effective Date:

**COMPANY Logo**

Revised:

Approved by: CISO Approved on: 00/00/20XX

Approved by: COO Approved on: 00/00/20XX

Approved by: Board of Directors Approved on: 00/00/20XX

# Purpose

The purpose of the Information Security Management Policy is to manage information security within COMPANY (“COMPANY”). This policy describes the process requirements to initiate and control the management of information security within COMPANY information systems. An Information Security Program that provides management direction and support for information security in accordance with business requirements and relevant laws and regulations will be established.

# This policy describes risk management requirements to include identification, quantification, and prioritization of risks against criteria for risk acceptance and objectives relevant to COMPANY. The results will guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks and to ensure they are managed in compliance with the Information Security Policy Master Plan.

# This policy requires:

# Senior Management support, direction, and commitment

# Establishing, approving, and maintaining Information Security Policies

# COMPANY’s ability to efficiently and effectively create, collect, process, control, and use business information assets

# COMPANY information is protected to a level which adequately reflects the business risk from unauthorized access, disclosure, modification or loss, and takes into account its value to COMPANY and its criticality or sensitivity

# COMPANY’s compliance with international, federal, state, local laws and regulations

# A Risk Management Strategy to identify, assess, quantify, and prioritize risks

# Risk Analysis

# Risk measurements to monitor information security risks

# Risk controls to safeguard the target risk level

# Scope

This policy applies to Users (employees, contractors, vendors, consultants, or other persons) having access to COMPANY computing assets or information. It applies to all systems used to conduct COMPANY business, and sets forth the information security risk management program. The scope of the security risk assessment can be either the entire COMPANY organization, parts of the infrastructure, an individual information system, specific system components, or services where this is practicable, realistic, and helpful.

This policy sets forth governance for information security which applies to any information that is created, processed, stored or transmitted during the normal course of business. The framework sets the basis for determining the potential risks and security measures needed to protect that information. It exists to protect COMPANY’s information network and infrastructure and must be adhered to.

# Roles and Responsibilities

## The RACI Chart below shows the assignment of functional and cross-functional activities. The roles are as follows:

| R - Responsible is the organizational title responsible for doing the work.A - Accountable is the organizational title for who is accountable for the work being done.C - Consulted is the organizational title that provides necessary information.I - Informed is the organizational title that receives information. **Milestone or Task** | Governance / Risk Management | Chief Information Security Officer | Information Security Organization / IT | Senior Management | Users |
| --- | --- | --- | --- | --- | --- |
| Management Commitment | C | C | R | A | I |
| Security Coordination | C | A | R | I | I |
| Identify Security Roles and Responsibilities | C | A | R | I | I |
| Develop Information Security Policies | C | A | R | I | I |
| Maintain Information Security Polices | C | A | R | I | I |
| External Parties Security | C | A | R | I | I |
| Risk Management Strategy | C | A | R | C | I |
| Risk Analysis | C | A | R | C | I |
| Risk Measurement | C | A | R | C | I |
| Risk Control | C | A | R | C | I |
| Security Coordination | C | A | R | I | I |
| Identify Security Roles and Responsibilities | C | A | R | I | I |
| External Parties Security | C | A | R | I | I |

# Policy Statements

# The Information Security Management Policy is established to provide reliable and consistent security services and protect information assets by implementing security controls to prevent the unauthorized disclosure, modification, insertion, deletion, or destruction. Information security policies define the requirements for the protection of information and technology from internal and external threats to confidentiality, integrity and availability.

Risk Management processes including security assessments, vulnerability, threat, and risk analysis, risk measurements, and risk control are performed at least annually.

This is accomplished via the following:

## Management Commitment

* + 1. Senior Management must:
    2. Ensure that information security goals are identified, meet COMPANY requirements, and are integrated in relevant processes
    3. Provide clear direction and visible management support for security initiatives;
    4. Ensure that the implementation of information security controls is coordinated across COMPANY
    5. Senior Management must:
    6. Set a clear policy direction in line with business objectives
    7. Demonstrate support for, and commitment to, information security through the issue and maintenance of Information Security Policies
    8. Approve the Information Security Policies
    9. Review the effectiveness of the implementation of the Information Security Policies
    10. Senior Management must:
    11. Assign security roles
    12. Actively support information security within COMPANY through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities
    13. Approve assignment of specific roles and responsibilities for information security across COMPANY
    14. Coordinate and review the implementation of security across COMPANY
    15. Provide the resources needed for information security
    16. Senior Management must initiate plans and programs to maintain information security awareness.

## Develop Information Security Policies

* + 1. The Information Security Organization must develop and document Information Security Policies; approved by Senior Management, published, and communicated to all Users and relevant external parties.
    2. The Information Security Organization must ensure that the Information Security Policies Master Plan states Senior Management’s commitment and sets out the COMPANY’s approach to managing information security.
    3. The Information Security Organization must ensure the Information Security Policies are communicated throughout COMPANY to Users in a form that is relevant, accessible, and understandable to the intended reader.

## Maintain Information Security Policies

* + 1. The Information Security Organization must ensure the Information Security Policies are reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.
    2. The Information Security Organization must own and have responsibility for the development, review, and evaluation of the Information Security Policies.
    3. The Information Security Organization must continually assess opportunities for improvement of COMPANY’s Information Security Policies and approach to managing the Information Security Program in response to changes to the COMPANY environment, business circumstances, legal conditions, or technical infrastructure.

## Risk Management Strategy

* + 1. The Information Security Organization must establish a Risk Management strategy that provides a quantitative assessment of the security risks.
    2. The Information Security Organization must define a framework which will outline COMPANY’s Risk Management processes.
    3. The Information Security Organization must perform the process of assessing risks and selecting controls a number of times to cover different parts of the organization or individual information systems.
    4. The Information Security Organization must employ a Risk Management strategy that includes a systematic approach of estimating the magnitude of risks (risk analysis) and a process of comparing the estimated risks against risk criteria to determine the significance of the risks (risk evaluation).
    5. The Information Security Organization must identify tools, processes, and metrics to be used in evaluating the risk to an asset.
    6. The Information Security Organization must perform risk analysis prior to granting third party access or implementing third party products or services.
    7. The Information Security Organization must perform risk analysis during the development life cycle to ensure security safeguards are designed into the system.
    8. The Information Security Organization must analyze planned technology applications prior to implementation in order to reduce negative impact to the existing infrastructure.
    9. The Information Security Organization must perform an analysis of the effort involved in implementing security safeguards and whether or not it is appropriate for the given risk level.

## Risk Analysis

* + 1. The Information Security Organization must perform periodic risk assessments to address changes in the security requirements and in the risk situation, e.g. in the assets, threats, vulnerabilities, impacts, the risk evaluation, and when significant changes occur.
    2. The Information Security Organization must perform risk assessments in a methodical manner capable of producing comparable and reproducible results.
    3. The Information Security Organization must ensure that all risk assessments have a clearly defined scope in order to be effective.
    4. The Information Security Organization must ensure that all computer systems, networks, and applications are periodically assessed for compliance with information security policies. This risk assessment must occur at least annually.
    5. The Information Security Organization must ensure that COMPANY’s business and security environment is assessed for threats and vulnerabilities. This risk assessment must occur at least annually.

## Risk Measurement

* + 1. The Information Security Organization must measure each risk and consider the treatment.
    2. The Information Security Organization must decide criteria for determining whether or not risks can be accepted. Risks may be accepted if, for example, it is assessed that the risk is low or that the cost of treatment is not cost-effective for COMPANY. Such decisions must be recorded.
    3. The Information Security Organization must initiate objective risk measurements and tests of security controls.
    4. The Information Security Organization must perform a baseline risk assessment on all new hardware/software prior to being put into production.
    5. The Information Security Organization must, on an annual basis, review security configurations and corresponding levels of risk acceptable to the business.
    6. The Information Security Organization must, on an annual basis, perform checks to ensure that security safeguards are implemented as required and are being properly used.
    7. The Information Security Organization must, or have a third party, perform a baseline system vulnerability scan and penetration test prior to a production rollout.
    8. The Information Security Organization must, or have a third party, perform system vulnerability and penetration tests annually.
    9. The Information Security Organization must monitor all systems and networks to ensure that they maintain the recommended security configurations consistent with the accepted level of risk.

## Risk Control

* + 1. The Information Security Organization must select and implement risk controls to meet the requirements identified by the risk assessment.
    2. The Information Security Organization must implement security safeguards necessary to properly control the security target risk level.
    3. The Information Security Organization must control risk in such a way that it does not expose COMPANY to unacceptable levels of risk.
    4. The Information Security Organization must implement risk controls that reduce risks to an acceptable level taking into account:

1. Requirements and constraints of national and international legislation and regulations;
2. Organizational objectives;
3. Operational requirements and constraints;
4. Cost of implementation and operation in relation to the risks being reduced, and remaining proportional to the organization’s requirements and constraints;
5. The need to balance the investment in implementation and operation of controls against the harm likely to result from security failures.
   * 1. The Information Security Organization must consider risk controls at the systems and projects requirements specification and design stage.
     2. The Information Security Organization and COMPANY Senior Management must understand that no set of controls can achieve complete security, and that additional management action should be implemented to monitor, evaluate, and improve the efficiency and effectiveness of risk controls to support COMPANY’s aims.

## Security Coordination

* + 1. The Information Security Organization must coordinate information security activities between representatives through-out COMPANY.
    2. The Information Security Organization must involve the cooperation and collaboration of Senior Managers, Users, System Administrators, application designers and developers, auditors, and security personnel, with specialist skills and knowledge in areas such as insurance, legal and regulatory issues, human resources, IT, governance, or risk management.

## Identify Security Roles and Responsibilities

* + 1. The Information Security Organization must clearly define all information security roles and responsibilities.
    2. The Information Security Organization must allocate information security roles and responsibilities in accordance with the Information Security Policies.
    3. The Information Security Organization must clearly identify roles and responsibilities for the protection of individual assets and for carrying out specific security processes. Responsibilities for the protection of assets and for carrying out specific security processes, such as business continuity planning, must be clearly defined.

## External Parties Security

* + 1. The Information Security Organization must identify risks to COMPANY’s information and information processing facilities from business processes involving external parties and implement appropriate controls before granting access.
    2. The Information Security Organization must address all identified security requirements before giving partners and other third parties access to COMPANY’s information or assets.
    3. The Information Security Organization must ensure that any outsourcing of IT services will not degrade the security posture of COMPANY as a whole.

# Compliance with Policies

# Use of COMPANY’s network, systems, hardware and applications represents the User’s consent to the terms of the policies described here, including consent for COMPANY to monitor and audit content and/or use. A User’s failure to comply with Information Security Policies may lead to disciplinary action to include one or more of the following:

* Oral and/or written warning or notification of violation to User(s) involved and supervisor(s)
* Suspension of network, system or application access or electronic communications privileges permanently or for a set period
* Repossession of electronic devices or hardware permanently or for a set period
* Electronic messages may be blocked or rejected if the message contains inappropriate or unauthorized content which is against COMPANY policy.
* Written warning to the User’s HR file
* Suspension from work
* Education course related to the infraction paid for by the User
* Regulatory discipline or censure
* Termination of employment

Users consent by reading this policy at time of hiring and at each annual evaluation by signing an Information Security Policy Acknowledgement form.

# Questions

Users are encouraged to contact the Chief Information Security Officer (CISO) or the Information Security Organization with any questions or concerns. It is critical for all Users to consult supervisors and/or the Information Security Organization about “red flags” (any suspicious activities giving rise to concerns about whether such activities meet or potentially violate Information Security Policies). All Users are encouraged to raise questions or concerns if they believe an information-security risk or leak is present.

# Disclaimers

COMPANY retains the right to:

* Restrict or revoke any User’s privileges to information, equipment or systems
* Inspect, copy, remove or otherwise alter any information, program, or other system resource that may undermine these objectives
* Take any other steps deemed necessary to protect COMPANY information or information systems

This right may be exercised with or without notice to the involved users. COMPANY disclaims any responsibility for loss or damage to information or software that results from COMPANY exercising its rights under Information Security Policies.

All documents, computing assets, and communications systems assets, including the email and phone systems, physically located at or pertaining to COMPANY are the property of COMPANY. COMPANY reserves the right to examine all information stored in or transmitted by these systems, subject to applicable law. Users should have no expectation of privacy associated with personal information and information stored in, created on, or sent through the COMPANY computer and communication systems.

# Definitions

The following terms are related to this Information Security Policy:

* **Electronic Communications**: Includes e-mail and instant messaging sent from or received by COMPANY equipment or sent or received, including with the addresses “dadco.com” or “Bloomberg.net.”
* **Information Security**: Includes the concepts, techniques, technical, administrative, and managerial measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, manipulation, modification, loss, or use.
* **Information Security Policy**: The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
* **Information Security Program**: Is the program, whose mission is to provide a core set of information security and privacy controls to ensure the confidentiality, reliability, integrity, availability and security of its corporate information (both electronic and paper) used enterprise-wide.
* **Non Disclosure Agreement (NDA)**: A contract whereby one promises to treat information confidentially and not give out information without proper authorization.
* **Requirement**: A condition or capability that must be met or possessed by a system or system component to satisfy a contract, standard, specification, or other formally imposed document.
* **Review**: Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives.
* **Risk Assessment**: A formal process that identifies what aspects of a system/process are critical to the business, how much validation is required for the system, does the automated system require validation and/or does the system require compliance with applicable laws and regulations.
* **Security**: The protection of computer hardware, software, and data from accidental or malicious access, use, modification, destruction, or disclosure. Security also pertains to personnel, information, communications, and the physical protection of computer installations.
* **Security Officer**: The person responsible for ensuring that security is provided for and implemented correctly.
* **Security Policy**: The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive data and facilities.
* **Security Assessment**: Evaluation of the vulnerability of a network and the possible threats to its security.
* **Service Level Agreement** **(SLA)**: An agreement between user and a supplier that provides support services. The SLA should unambiguously define the system to be supported, define how the service is to be provided, and provide a means of measuring the performance of the support service being delivered against the requirements laid out in the agreement.
* **Users**: Any employees, contractors, vendors, consultants, or other persons having access to COMPANY computing assets or information.