Information Security Policy Library

(Abridged Version 10/2021)

Policy Index

A01 Information Security Program

Policy Statement

All information collected, processed, stored on, or transmitted over Maximizer computer systems and networks will be treated as a Maximizer corporate asset. It is the policy of Maximizer to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of our sensitive information assets. Maximizer will maintain an information security program to control risks associated with access, use, storage, sharing, and destruction of sensitive customer and financial information. This program will document minimum standards of behavior for staff, contractors and service providers and include clear guidance for the day-to-day operations of Maximizer. At a minimum, the program must include:

- Risk Assessment
- Risk Mitigation and Management
- Monitoring and Reporting
- Audit
- IT Oversight and Program Adjustment
- Vendor Management

Policy Development

A critical part of our risk mitigation plan is to provide policies and risk mitigation guidelines to our staff and partners. We will leverage best practices including the ISO framework to develop policies and document security procedures to meet operational risk mitigation objectives as well as compliance with customer privacy expectations and other regulatory requirements. At a minimum, the InfoSec Committee and CTO will review and approve required changes to policies and standards at least once per year.

A02 Acceptable Use

Policy Statement

Computers and networks can provide access to information resources both internal and external to Maximizer networks. To ensure this information is handled responsibly, users are to respect the rights of other users, protect the confidentiality and integrity of the systems and related physical resources, and observe all relevant laws, requirements, and regulations. Failure to comply or act in accordance with this policy will result in sanctions, up to and including termination of employment. Specific guidance for end user acceptable use may be found in the standards established for this policy.

Formal acknowledgement and understanding of Maximizer's acceptable use policies and standards will be a mandatory requirement for all users prior to obtaining access to company information resources.

Standards

The following standards are provided to establish the acceptable use of Maximizer technology for Applicable Users:

- Obtaining Access
- Security
- Acceptable Use Standards for:
    - Maximizer Systems and Networks
    - Email
    - Internet Access
    - Remote Access
    - Telephone Access
    - Social Media

A03 Risk Management Program

Policy Statement

The Information Security Officer (ISO) will develop and maintain an Information Security Risk Management Process to frame, assess, respond, and monitor risk. Guidance for this process will be based on the International Organization for Standardization ISO 27001 framework and specific security regulations e.g. SOC, PCI-DSS, etc. The risk management process will be designed to assist Maximizer maintain compliance with regulatory requirements, federal and provincial laws.

Risk management will involve all Maximizer stakeholders. The ISO will engage with our stakeholders, departments, contractors, and partners to increase awareness and communication of risk and to identify methods to integrate risk management in our culture, projects, processes, strategic and operational planning. Expectations for all stakeholders will be open, clear, and transparent.

The ISO will identify, categorize, prioritize and report risks based on the probability and potential impact to the environment if confidentiality, availability and/or integrity is compromised. The risk evaluation will be uniform and consistent all departments.

Risk Management Roles and Responsibilities

Role	Responsibilities
Executive Leadership	• Approves Capital Expenditures for Information Security • Communication Path to Stakeholders
CTO	• Sponsors the ISO to ensure the information security risk process is followed for Maximizer processes and projects
ISO	• Will maintain the risk register • Communicate information security risks to Executive Leadership • Will report annually to Executive Leadership on risks that need to be addressed to bring risk to acceptable level • Responsible for conducting risk assessments, documenting the identified threats and the likelihood of occurrence. • Develop policy, procedure and solutions to mitigate identified risk to an acceptable level.
Department Managers	• Responsible for the implementation of risk mitigating controls and ensure they are properly maintained
Maximizer Staff, Contractors, Partners	• Acting at all times in a manner which does not place at risk the health and safety of themselves, other person in the workplace, and the information and resources they have use of • Helping to identify areas where risk management practices should be adopted • Taking all practical steps to minimize Maximizer's exposure to contractual and regulatory liability.

A.5 Information Security Policies

Policy Standards - Creation, Revision, Review & Approval

Creation

- Maximizer creates and maintains an Information Security Policy document (and supporting Information Security Program Manual) and information security standards that describe how the policy will be met.
- Maximizer ensures the Information Security Policy will exist/be published in Maximizer infosec repository".
- Maximizer policies and standards follow a standard template.
- All Maximizer policies and standards are created in alignment with documentation standards for security documents.

Revision

- Maximizer ensures that policy documents are revised when the underlying set of principles changes, or to correct information, or to enhance the effectiveness of the document.
- Maximizer ensures that standard documents are revised when the underlying policy changes, to correct information, or to enhance the effectiveness of the standard statements.

Review

- Maximizer ensures policy and standard documents are reviewed when revised, or annually at a minimum if no revisions occur.
- The Security Assurance team reviews the original creation and subsequent updates to policies and standards.
- Maximizer ensures that a content owner or department owner (director or above) is identified for the relevant policy or standard.

Approval

- Maximizer ensures that policies and standards become effective the date of approval of the policy document, unless otherwise noted within the document.
- The CTO ensures approvals are documented with the full name of the approver and date of approval.
- The CTO manages the annual review and approval process to allow for updates and material changes to policies and standards.

Stakeholder Engagement

- Relevant stakeholders are engaged throughout the creation, revision, review and approval process as appropriate to provide business insights into technical limitation, process deficiencies, or environmental constraints that may limit effectiveness of a policy or standard.
- Legal may review policies and standards published for compliance with regulatory requirements and contractual obligations.

Communications

- Maximizer personnel are made aware of policies and standards and have access to the documentation.
- Maximizer ensures that all policies and standards are made available on Maximizer infosec repository".

Compliance

- The IT Department and Department Managers monitor compliance to policies, standards, and controls either manually or automatically.
- The CTO provides control owners, in case of non-compliance, with feedback and a corrective action plan.

A.6 Organization of Information Security

Policy Statement

In order to effectively implement and enforce Maximizer's information security program, specific roles and responsibilities are assigned to the Senior Management, the IT Steering Committee, IT staff and full-time and temporary staff. Senior Management will periodically assess the capabilities and expertise of existing staff and outside vendors and to ensure that all systems and services are effectively managed and that responsibilities have been assigned to both accomplish security program objectives as well as segregate roles to assure adequate governance and oversight. As well, Maximizer will maintain contact with special interest groups and authorities and security will be addressed in all projects.

Standards:

- Information Security Roles & Responsibilities – to include:
  - CTO (Chairperson)
  - IT Manager
  - Information Security Officer
  - Accounting
  - HR
  - Legal
  - Other Business Departments as Necessary
- Segregation of Duties
- Contact with Authorities
- Contact with Special Interest Groups
- Information Security in Project Management

A.7 Human Resource Security

A.7.1 Prior to Employment (Screening)

Policy Statement

Prior to Employment a pre-employment screening process must be undertaken by Maximizer prior to offering employment, to a new employee. Checks must include at least the following:

- Identity checks (driver's license, passport, bank account in the same name as the employee, etc.)
- Reference checks
- Confirmation of academic or professional qualifications as appropriate
- Criminal records checks for senior positions or positions with access to sensitive information (e.g. finance, IT administration)

If the employee is being hired through a third party or staffing agency, screening checks in line with those stated above must be implemented by that agency.

Information gathered on potential employees must be secured by all applicable laws and regulations. Access must be limited to 'need to know' basis.

All staff must agree to comply with Maximizer IT Security Policy and Standards prior to being granted access to Maximizer Information, Communication and Technology systems. Also, staff are required to sign a Non-Disclosure Agreement if their role requires access to sensitive information.

Standards:

- Screening
- Terms and Conditions of Employment

A.7.2 During Employment

Policy Statement

Maximizer recognizes that our staff is our greatest resource in maintaining an effective level of security. At the same time, internal threats can create the greatest risks to information security. No security program can be effective without maintaining employee awareness and motivation.

Every Maximizer employee, contractor, service provider, and vendor is responsible for systems security to the degree that the function requires the use of information and associated systems. Fulfillment of security responsibilities is mandatory, and violations of security requirements may be cause for disciplinary action, up to and including dismissal, civil penalties, and criminal penalties.

All positions interacting with Maximizer information resources must be required to undergo formal processes for access granting, change, and termination. Those positions working with especially sensitive information or powerful privilege must be analyzed to determine any potential vulnerability associated with work in those positions.

Standards:

- Management Responsibilities
- Information Security Awareness, Education and Training
- Disciplinary Process

A7.3 Termination & Change of Employment

Policy Statement

All positions interacting with Maximizer information resources must be required to undergo formal processes for access granting, change, and termination. Those positions working with especially sensitive information or elevated privileges must be analyzed to determine any potential vulnerability associated with work in those positions.

Standards:

- Termination or Change of Employment Responsibilities

A.8 Asset Management

A.8.1 Responsibility for Assets

Policy Statement

Maximizer's IT assets are critical to productivity and corporate success. Effective IT asset management practices are essential.

Standards:

- Inventory of Assets
- Software Inventory and Updates
- System and Network Diagrams
- Ownership of Assets
- Acceptable Use of Assets
- Return of Assets

A.8.2 Information Classification

Policy Statement

Maximizer has established a framework for classifying information based on its level of sensitivity, value and criticality to the company. Classification of data will aid in determining baseline security controls for the protection of data.

All Applicable Users share in the responsibility for ensuring that Maximizer information assets receive an appropriate level of protection by observing this Information Classification policy:

- Managers or information 'owners' shall be responsible for assigning classifications to information assets according to the standard information classification system presented below.
- Where practicable, the information category shall be embedded in the information itself.
- All Applicable Users shall be guided by the information category in their security-related handling of Maximizer information.

Standards:

- Classification of Information
- Labelling of Information
- Handling Assets

A.8.3 Media Handling

Policy Statement

Maximizer has established a framework for classifying information based on its level of sensitivity, value and criticality to the company. Classification of data will aid in determining baseline security controls for the protection of data.

All Applicable Users share in the responsibility for ensuring that Maximizer information assets receive an appropriate level of protection by observing this Information Classification policy:

- Managers or information 'owners' shall be responsible for assigning classifications to information assets according to the standard information classification system presented below.
- Where practicable, the information category shall be embedded in the information itself.
- All Applicable Users shall be guided by the information category in their security-related handling of Maximizer information.

Standards:

- Management of Removable Media
- Disposal of Media
- Physical Media Transfer

A.9 Access Control

A.9.1 Business Requirements of Access Control

Policy Statement

Access to Maximizer systems and data on a "business need-to-know" basis.

Standards:

- Access Control Policy
- Access to Networks & Network Services

A.9.2 User Access Management

Policy Statement

Protecting access to IT systems and applications is critical to maintain the integrity of Maximizer's technology and data and to prevent unauthorized access to such resources.

Access to Maximizer systems must be restricted to only authorized users or processes, based on the principle of strict need to know and least privilege.

Standards:

- User Registration and De-registration
- User Access Provisioning
- Management of Privileged Access Rights
- Management of Secret Authentication Information of Users
- Review of User Access Rights
- Removal or Adjustment of Access Rights

A.9.3 User Responsibilities

Policy Statement

Access to Maximizer systems must be restricted to only authorized users or processes, based on the principle of strict need to know and least privilege. Users are obligated to keep their authentication information secret.

Standards:

- Use of Secret Authentication Information

A.9.4 System and Authentication Access Control

Policy Statement

Access to Maximizer systems must be restricted to only authorized users or processes, based on the principle of strict need to know and least privilege. Users are obligated to keep their authentication information secret.

Standards:

- Information Access Restriction
- Secure Log-on Procedures
- Password Management System
- Use of Privileged Utility Accounts
- Access Control to Program Source Code

A.10 Cryptography Controls

Policy Statement

Cryptographic controls play a significant role in the system of controls that Maximizer employs to protect its data assets. Toward this end, the CTO will establish and maintain a Cryptographic Controls Program aligned to the Information Classification Policy. The program will establish standards for minimum encryption strength for data in each data classification, when cryptographic controls are appropriate, encryption key management, and outgoing transmission identity validation. This program addresses information from end to end while in transit and as well as storage, both inside and outside Maximizer networks.

Standards:

- Policy on the Use of Cryptographic Controls
- Key Management

A.11 Physical and Environmental Security

Policy Statement

Physical access to facilities, data centers, systems, networks and data at Maximizer will be limited to those authorized personnel who require access to perform assigned duties. Where systems are deployed in areas where controls may not completely restrict access to only authorized personnel, monitoring controls will be deployed to identify unauthorized access to systems, network, and data.

In addition to access controls, physical safeguards will be deployed to protect sensitive systems and data from fire, theft or other hazard.

Standards for Secure Areas:

- Physical Security Perimeter
- Physical Entry Controls
- Securing Offices, Rooms and Facilities
- Protecting Against External and Environmental Threats
- Working in Secure Areas
- Delivery and Loading Areas

Standards for Equipment:

- Equipment Siting and Protection
- Supporting Utilities
- Cabling Security
- Equipment Maintenance
- Removal of Assets
- Security of Equipment and Assets Off-Premises
- Security Disposal or Reuse of Equipment
- Clear Desk and Clear Screen Policy

A.12 Operations Security

A.12.1 Operational Procedures and Responsibilities

Policy Statement

The Maximizer team is committed to operational security. Activities include protection against malware, logging and monitoring, control of operating system software, preventing the exploitation of technical vulnerabilities and ensuring that audit activities on operational systems is minimized.

Standards:

- Documented Operating Procedures
- Change Management
- Capacity Management
- Separation of Development, Testing and Operational Environments
- Systems Development Life Cycle

A.12.2 Protection from Malware

Policy Statement

This policy is designed to prevent viruses, malware and/or malicious code from infecting Maximizer's computing devices and network. By preventing infection, data, files, and resources will also be protected.

Standards:

- Controls Against Malware

A.12.3 Back-up

Policy Statement

The CTO and IT Manager must define and document backup and recovery processes that consider the confidentiality, integrity and availability requirements of information and information systems. Backup and recovery processes must comply with:

- Maximizer business continuity plans;
- Standards, policy, legislative, regulatory and other obligations; and
- Records management requirements.

Standards:

- Information Back-up

A.12.4 Logging and Monitoring

Policy Statement

Information systems must be monitored, and information security events recorded to detect unauthorized access to information and information systems. The CTO and IT Manager must define and document logging and monitoring processes that comply with Maximizer policies.

Standards:

- Event Logging
- Protection of Log Information
- Administrator and Operator Logs
- Clock Synchronization

- Intrusion Protection and Prevention

A.12.5 Control of Operational Software

Policy Statement

The installation of software on operational information systems must be controlled and monitored.

Standards:

- Installation of Software on Operational Systems

A.12.6 Technical Vulnerability Management

Policy Statement

To support technical vulnerability management, the IT Department must maintain an inventory of information assets in accordance with the Asset Management Security Policy.

Standards:

- Management of Technical Vulnerabilities
- Restrictions on Software Installation

A.12.7 Information Systems Audit Considerations

Policy Statement

All audit activities on operational systems must be pre-approved, defined and documented.

Standards:

- Management of Technical Vulnerabilities

A.13 Communication Security

A.13.1 Network Security Management

Policy Statement

The IT Department must ensure that networks (in-house or 3rd party vendors) are managed and controlled to protect information in systems and applications.

Standards:

- Network Controls
- Security of Network Services
- Segregation of Networks

A.13.2 Information Transfer

Policy Statement

The IT Department must ensure that information transfer is done in a secure manner.

Standards:

- Information Transfer Policies and Procedures
- Agreements of Information Transfer
- Electronic Messaging
- Confidentiality or Non-Disclosure Agreements

A.14 System Acquisition Development and Maintenance

A.14.1 Information Security Requirements Analysis and Specification

Policy Statement

Security considerations should happen from the earliest possible opportunity to ensure that the correct requirements are identified before solution selection commences. The security requirements should be documented and agreed so that they can be referenced as the solution is procured or developed.

Standards:

- Information Security Requirements Analysis & Specification
- Securing Application Services on Public Networks
- Protecting Application Services Transactions

A.14.2 Security in Development and Support Processes

Policy Statement

Security considerations for systems and application development should happen from the earliest possible opportunity to ensure that the correct requirements are identified before solution selection commences. The security requirements should be documented and agreed so that they can be referenced as a solution is procured and/or developed.

Standards:

- Secure Development Policy
- System Change Control Procedures
- Technical Review of Applications After Operating Platform Changes
- Restrictions on Changes to Software Packages
- Secure Systems Engineering Principles
- Secure Development Environment
- Outsourced Development
- System Security Testing
- System Acceptance Testing

A.14.3 Test Data

Policy Statement

It is imperative that test data used in development and testing is not inadvertently exposed to potential loss, damage, or compromise.

Standards:

- Protection of Test Data

A.15 Supplier Relationships

A.15.1 Information Security Policy for Supplier Relationship

Policy Statement

Maximizer must implement information security protocols to mitigate risks associated with 3rd party suppliers having access to Maximizer assets.

Standards:

- Information Security Policy for Supplier Relationships
- Addressing Security Within Supplier Agreements
- Information and Communications Technology Supply Chain

A.15.2 Supplier Service Delivery Management

Policy Statement

Maximizer must establish rules for monitoring and review of supplier services.

Standards:

- Monitoring and Review of Supplier Services
- Managing Changes to Supplier Services

A.16 Information Security Incident Management

Policy Statement

Incident management responsibilities and procedures must be established to ensure a quick, effective and orderly response to information security incidents. The CTO, ISO and IT Manager are responsible to ensure the following procedures are developed and implemented:

- Incident response planning and preparation;
- Monitoring, detecting, analyzing and reporting of information security events and incidents;
- Logging incident management activities;
- Handling of forensic evidence;
- Assessment of and decision on information security events and assessment of information security weaknesses;
- Response and recovery from an incident; and
- Learning from the incident.

A.17 Information Security Aspects of Business Continuity Management

A.17.1 Information Security Continuity

Policy Statement

Information systems must be implemented with redundancy sufficient to meet availability requirements:

- The CTO, IT Manager and the Management Team must identify business requirements for the availability of information systems. When the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures must be considered.
- Where applicable, redundant information systems must be tested to ensure the failover from one component to another works as intended.

A.17.2 Redundancies

Policy Statement

Information systems must be implemented with redundancy sufficient to meet availability requirements:

- The CTO, IT Manager and the Management Team must identify business requirements for the availability of information systems. When the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures must be considered.
- Where applicable, redundant information systems must be tested to ensure the failover from one component to another works as intended.

Standards:

- Availability of Information Processing Facilities

A.18 Compliance

Information Security Reviews

Policy Statement

Maximizer takes the security of our staff, customers, business and assets seriously. To this end, we will regularly review of our security risks and controls and our compliance with, and enforcement of, published security policies.

Standards:

- Independent Review of Information Security
- Compliance with Security Policies and Procedures
- Technical Compliance Review