Information Technology and Information Technology Security Policy

Approved by the board on
November 6, 2020

Summary:

The purpose of the Information Technology and Information Technology Security Policy is to regulate IT and IT security within the Corporation in order to meet business and operational requirements in the financial, legal, and accounting contexts. The Policy outlines the responsibilities and roles of various people within the Corporation in maintaining and protecting Midas Gold's IT systems and its data in accordance with its obligations as a public company.

A. INTRODUCTION

Entities within Midas Gold Corp. ("Midas Gold" or the "Corporation") shall carry out internal work processes in a quality-assured and cost-effective way. The users shall receive high quality service for the information technology ("IT") systems – including documentation, training, and support. Midas Gold shall strive to harmonize and integrate different systems within the organization.

The Corporation shall work with cost-effective solutions for the Corporation's overall IT needs.

B. PURPOSE OF THIS POLICY

The purpose of this Policy is to regulate IT and IT security within the Corporation in order to meet business and operational requirements in the financial, legal, and accounting contexts. In terms of both operational reliability and functionality, our consultants and staff directly depend on the integrity of our IT systems. Therefore, our systems shall also enable risk management and security routine requirements from external inspection authorities to be adhered to. In order to fulfill these requirements, guidelines must be in place defining progress and process of work to be completed. This Policy describes these requirements.

This Policy affects choice of system, data protection, purchasing routines and user services.

C. RESPONSIBILITY

The President of Midas Gold is ultimately responsible for the operational continuity of IT and IT security at the Corporation. Additionally, it is management's responsibility to ensure a well-functioning organization for this work. To ensure the business needs for protection and security are fulfilled, management shall initiate and support the security work with necessary resources.

The local managers of the Corporation are responsible for the compliance with the rules and requirements established in this Policy. These responsibilities include:

1. allocating resources to ensure that rules for IT and IT security are communicated, applied and maintained; and

2. ensuring that sufficient security responsibilities are established and communicated - including appointing system owners to the information systems.

System owners are obligated to ensure adherence and compliance with all requirements in this Policy. Additionally, local managers are required to ensure that this Policy is complied with.

Compliance with this Policy shall also apply to contractors, consultants and outsourced service providers that connect into or use the Corporation's IT systems.

D. ROLES

The Chief Financial Officer ("CFO") of the Corporation has overall responsibility for the coordination of IT and IT security work in the Corporation. These responsibilities include:

1. being responsible for the Corporation's directive for IT and IT security – including: ensuring that rules governing IT security are continuously developed, communicated and updated as required by changes in IT and IT security best practice;

2. maintaining a plan for IT security;

3. ensuring that the information security rules and procedures communicated to all appropriate staff and making all reasonable efforts to ensure the information security rules and procedures are adhered to;

4. reporting IT security incidents and breaches to management; and

5. monitoring the compliance with this Policy and providing regular status reports to management.

The local IT personnel within the Corporation are responsible for fulfillment of the rules and requirements in this Policy. These responsibilities include:

1. ensuring that the local systems and network of the subsidiary fulfills the central IT security requirements and directives;

2. organizing the IT security responsibilities according to this Policy;

3. ensuring that the system owner's requirements regarding availability, confidentiality and integrity are met;

4. initiating reviews of IT security within the entity and ensure that identified weaknesses are appropriately addressed and/or reported; and

5. following up on incidents and breaches to ensure appropriate actions for risk mitigation.

The system owners of the Corporation are responsible for security, confidentiality, integrity and availability. The system owners are responsible for performing risk analysis for the system and its information.

E. REQUIREMENT SPECIFICATION

1. Systems

The Corporation shall work with well recognized systems from reliable vendors.

All entities within Midas Gold shall perform risk assessments on a regular basis.

2. Data Protection

Three main risk areas shall be considered regarding data protection:

(a) Confidentiality;

(b) Integrity; and

(c) Availability.

2.1 ***Access Management***

Access to systems and information shall be managed in a formal way and be based on security requirements.

Before physical and logical access to the Corporation's information and IT systems is granted, all personnel of the Corporation and Midas Gold's external resources (consultants and contractors) shall sign a Confidentiality Agreement.

Access to all systems shall be protected by passwords or biometric authentication with the level of access controlled.

2.2 ***Security Classification***

Every system and its information shall be classified based on data content. The security classification levels are:

(a) Confidential;

(b) Internal; and

(c) Public.

2.3 ***Information Security***

Ensure existence of proper routines for:

(a) Backups of data;

(b) Consistency of data; and

(c) Availability of data.

All system infrastructures within the Corporation shall be configured to protect the Corporation's data and prevent unauthorized access.

2.4 ***System Availability***

All IT systems and stored data shall be adequately secure and readily available within the Corporation.

2.5 ***Change Management***

Any changes to applications and critical IT infrastructure within the Corporation shall be conducted through formalized routines.

2.6 ***Physical Access to Premises***

All access to premises of the Corporation shall be restricted by appropriate physical entry controls to ensure that only authorized personnel are allowed access.

2.7 ***Logging***

System logging shall be activated on all IT systems to trace each user's access and activity in the system.

2.8 ***Incident Handling***

IT security events leading to an incident or breach shall be reported and documented.

2.9 ***Disaster Recovery***

Disaster recovery plans shall be documented and tested for critical for processes and systems.

2.10 ***Archiving***

Documents and electronic records required to support any of the Corporation's regulatory requirements shall be archived for at least seven years.

F. USER SERVICE

Users shall receive sufficient support for using the IT environment. This includes:

(a) User manuals;

(b) Training; and

(c) Application support.

G. COMPLIANCE

The Corporation's CFO shall ensure that the Corporation's employees comply with this Policy.

In order to monitor IT security, analyses shall be carried out to support the evaluation of compliance with this Policy through self-assessments or independent reviews, performed on a regular basis and/or when major changes occur. Moreover, status shall be reported on a regular basis to the Corporation's management.

H. EXEMPTIONS TO THIS POLICY

There may be cases in which this Policy cannot be fulfilled in all respects. If a system does not meet the requirements and guidelines described in this Policy, an exemption report shall be used.