Perpetua Resources

Information Technology and Information Technology Security Policy

Approved by the board on February 8, 2024

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 Perpetua Resources IT systems and its data in accordance with its obligations as a public company.

A. INTRODUCTION

Entities within Perpetua Resources Corp. ("Perpetua Resources" 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. Perpetua Resources 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 govern 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 also enable risk management and security routine requirements from external inspection authorities to be adhered to. In order to fulfill these requirements, guidelines are 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 Perpetua Resources 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. identification and oversight of system owners;

4. approval of new IT systems and services;

5. banning of IT systems and services;

6. ensuring that the information security rules and procedures communicated to all appropriate staff, including regular training, and making all reasonable efforts to ensure the information security rules and procedures are adhered to;

7. reporting IT security incidents and breaches to management

8. overseeing risk management of IT systems/security; and

9. 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. by applying the formal risk management process, initiate reviews of IT systems/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 with final approval coming form the CFO. Directives from the CFO or their delegate can ban the use of specific systems or specific system usage.

The CFO, IT personnel, and system owners within Perpetua Resources shall perform formal risk assessments on a regular basis. The risk assessments shall drive the construction and evolution of the IT ecosystem.

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 best practices. Access to systems and information shall be provided according to job responsibility under a least-privilege model.

Prior to granting physical and logical access to the Corporation's facilities and IT systems that contain confidential or internal data types, a Confidentiality Agreement must be submitted to IT for both personnel of the Corporation, including subsidiaries, and external parties (consultants and contractors. The Human Resources department or Company Sponsor will submit the signed Confidentiality or Nondisclosure Agreement to IT along with the request for resource access.

Access to all systems that contain confidential or internal data shall be protected by passwords and two factor authentication when applicable following a least privilege model. User access shall be promptly removed or updated to reflect changes in job roles or termination. Guest accounts shall be limited and monitored with quarterly reauthorization from a company sponsor. Quarterly reviews of user access rights shall be conducted by IT personnel to ensure appropriate access levels.

Access to systems that contain federally regulated data associated with government contracts requires background checks and specialty training on functioning in those data systems in addition to confidentiality agreements.

2.2 *Security Classification*

Every system and its information shall be classified based upon the highest data content type stored. The security classification levels in descending order are:

(a) Confidential;

(b) CUI (or other federally defined data classifications related to government contracting);

(b) Internal; and

(c) Public.

2.3 *Information Security*

Ensure existence of proper routines for:

(a) Backups of data;

(b) Consistency of data;

(c) Availability of data; and

(b) Recovery 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. Such formalized routines should include a plan that describes the process of reverting the environment to its original configuration if the change does not go as intended and a set of planned tests to verify that the change accomplished what it was supposed to do and does not adversely affect other system components.

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, and all logs shall be regularly reviewed to monitor the activities of users, administrators and system operators.

2.8 *Incident Handling*

IT security events leading to an incident or breach shall be reported and documented and any failure of a security control shall be followed up with a risk assessment to determine whether additional measures are warranted to resolve the failure.

2.9 *Disaster Recovery*

Disaster recovery plans shall be documented and tested for critical processes and systems and shall set forth how and when data will be recovered and restored following any disaster, including systematic backup and recovery procedures and strategies for implementing these procedures.

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.

2.11 *Security Awareness and Training*

All employees are required to complete quarterly cybersecurity training. Training programs shall cover best practices, policies, and emerging threats. Failure to complete required training may result in revocation of access to Corporate IT systems.

F. USER SERVICE

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

(a) User manuals;

(b) Regular training; and

(c) Application support.

G. COMPLIANCE

The Corporation shall comply with all relevant laws, regulations, and industry standards related to information security. Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or legal action. 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 should be used.

Exemptions should be documented and records maintained for 7 years.

I. CHANGES TO THIS POLICY

This Policy will be reviewed on a regular basis, at least annually, by the Board of Directors of the Corporation (the "Board") to confirm that it describes reasonable security measures and appropriate protections required by law, consistent with industry standards. Any changes to this Policy require approval of the CFO and must be adopted by the Board before they become effective.