Approved by the BOD based on CAPIC By-Laws and BOD Policy provisions.
Approved on December 3,2024

CAPIC IT Governance, and Risk Mitigation Policy

1. Purpose and Scope

Purpose

The purpose of this Policy is to establish guidelines and procedures for managing and aligning IT resources and activities with the strategic goals of CAPIC. By adhering to this comprehensive IT governance, and Risk Mitigation Policy, CAPIC ensures the security of its IT infrastructure, compliance with legal requirements, and the safety of its data and resources. All employees are expected to understand and comply with these policies to contribute to a secure and productive work environment.

This policy aims to:

- Maintain the security and integrity of CAPIC's IT infrastructure.
- Ensure compliance with legal, regulatory, and industry-specific requirements.
- Support productivity by providing clear guidelines for the use of IT resources.
- Minimize risks related to IT operations, including data breaches, unauthorized access, equipment loss.
- Outline procedures for responding to IT-related incidents effectively and
- ensure effective decision-making and value creation through the use of technology.

Scope

This policy applies to all CAPIC employees, including full-time and part-time employees, directors and volunteers, contractors, interns, consultants, third-party vendors who interact with the organization's IT infrastructure, and any other individuals with access to CAPIC's IT resources. It covers all IT systems, networks, devices, data, and communication tools owned, leased, or used by CAPIC, including those used by remote workers and mobile employees.

2. Security Requirements

Device Security

- **Personal and Company-Issued Devices:** All personal and company-issued devices must be secured according to CAPIC's security standards. This includes mandatory use of anti-virus software firewalls, and regular updates.
- **Anti-virus and Anti-Malware:** All devices must have approved anti-virus and anti-malware that are installed and configured for automatic updates and scans.
- **Patching and Updates:** Devices must be configured for automatic updates to ensure the latest security patches are applied promptly.
- **Physical Security:** Employees, including full-time and part-time employees, directors and volunteers, contractors, interns, consultants, must protect devices from theft or loss by using security locks, keeping devices under supervision, and securing devices in locked cabinets or drawers when not in use.

Data Protection

- **Data Handling:** Employees, including full-time and part-time employees, directors and volunteers, contractors, interns, consultants, must handle sensitive data with care, ensuring it is stored securely,
  encrypted when necessary, and only accessible to authorized personnel.
- **Encryption:** Sensitive data must be encrypted both at rest and in transit, using CAPIC-approved encryption standards.
- **Secure File Sharing:** Data sharing must be conducted through secure channels (e.g., CAPIC-approved file-sharing services with end-to-end encryption).
- **Data Disposal:** Proper disposal of data must be followed, including digital data shredding and physical destruction of storage media.

Network Security

- **Secure Connections:** All network connections must be secure, utilizing CAPIC-approved methods such as Virtual Private Networks (VPNs) , which are exclusively available to individuals using CAPIC-owned devices for remote access. Public Wi-Fi networks should be avoided for work purposes unless connected through a VPN.

- **Network Segmentation:** CAPIC's network is segmented to restrict access based on the principle of least privilege.
- **Firewall Configurations:** Firewalls must be configured to protect CAPIC's network from unauthorized access and must be reviewed regularly.

3. Access Control

Authentication

- **Strong Password Policies:** Employees, including full-time and part-time employees, directors and volunteers, contractors, interns, consultants, must use strong passwords that meet CAPIC's complexity requirements, including a minimum length, use of special characters, and regular updates.
- **Multi-Factor Authentication (MFA):** MFA is required for accessing all CAPIC systems and applications, providing an additional layer of security.
- **Secure Login Procedures:** Employees, including full-time and part-time employees, directors and volunteers, contractors, interns, consultants, must follow secure login procedures, including logging out of devices when not in use and avoiding shared or public computers for accessing CAPIC systems.

Authorization

- **Access Levels:** Access levels are defined based on the employee's role and need-to-know basis, ensuring employees only have access to necessary information.
- **Role-Based Access Control (RBAC):** CAPIC utilizes RBAC to ensure that employees have access only to the data and systems necessary for their job functions.
- **Regular Access Reviews:** Access privileges are reviewed periodically to ensure they remain appropriate based on employees' roles and responsibilities.

4. Use of Company Resources

Hardware and Software

- **Approved Use:** Employees, including full-time and part-time employees, directors and volunteers, contractors , interns, consultants, must use company-issued devices and software strictly for work purposes. Personal use is restricted and monitored to ensure compliance with this policy.

- **Software Installation:** Employees, including full-time and part-time employees, directors and volunteers, contractors, interns, consultants, are prohibited from downloading or installing unauthorized software to prevent malware and unauthorized software use. All software installations must be approved by IT.
- **Equipment Maintenance:** Employees, including full-time and part-time employees, directors and volunteers, contractors, interns, consultants, are responsible for the proper use and maintenance of company-issued equipment and must report any issues or damages to IT immediately to the administrative coordinator.

IT Support

- **IT Issue Reporting:** Remote workers can access IT support exclusively through CAPIC's designated IT contractor. For assistance with laptops, Office 365, or other IT-related concerns such as hardware malfunctions, software errors, or security issues, employees, including full-time and part-time employees, drectors and volunteers, contractors, interns, consultants, must promptly contact IT contractor . All issues should be reported to IT Team to ensure efficient handling and timely resolution.

5. Communication Tools and Protocols

Approved Tools

- **Communication Tools:** Employees, including full-time and part-time employees, directors and volunteers, contractors, interns, consultants, are required to use CAPIC-approved communication andcollaboration tools (e.g., Microsoft Teams, Slack, Zoom) for all work-related communications.
- **Tool Usage Guidelines:** Employees, including full-time and part-time employees, directors and volunteers, contractors, interns, consultants, must follow usage guidelines for each tool, including proper setup, maintenance of communication channels, and adherence to security settings.

Communication Etiquette

- **Professional Conduct:** Employees, including full-time and part-time employees, directors and volunteers, contractors, interns, consultants, must maintain professional conduct during all communications, adhering to CAPIC's guidelines for respectful and constructive communication.
- **Response Times:** Employees, including full-time and part-time employees, directors and volunteers, contractors, interns, consultants, are expected to respond to work-related communications withinestablished time frames, ensuring collaboration and productivity.

6. AI Usage Policy:

The use of AI tools at CAPIC must align with organizational guidelines and receive prior approval. AI tools are to be utilized exclusively by staff members who have been granted access. These tools are intended to enhance productivity, streamline workflows, and support CAPIC's objectives, while ensuring compliance with privacy, security, and ethical standards, non-discrimination, and must not utilize AI to make employment decisions without additional CAPIC review and approval. Staff are required to use AI responsibly and only for purposes approved by the organization.

7. Productivity and Performance

Work Hours

- **Expected Work Hours:** Employees must adhere to their scheduled work hours and be available for communications and meetings during these times. Any deviations must be communicated to supervisors.
- **Time Tracking:** Employees are required to accurately track their working hours using CAPIC-approved time-tracking tools.

Performance Monitoring

- **Monitoring Tools:** CAPIC uses various tools to monitor productivity and performance, including project management software, time-tracking systems, and regular check-ins with supervisors.
- **Performance Evaluations:** Regular performance evaluations will be conducted to assess productivity, adherence to policies, and overall contribution to team goals.

8. Training and Awareness

Security Awareness Training

- **Mandatory Training:** All employees, must complete mandatory cybersecurity awareness training during onboarding and at regular intervals thereafter.
- **Ongoing Education:** CAPIC provides ongoing education opportunities on cybersecurity best practices, including phishing prevention, secure data handling, and incident response.

Policy Acknowledgment

- **Acknowledgment Process:** Employees, including full-time and part-time employees, directors and volunteers, contractors, interns, consultants, must acknowledge understanding and compliance with the IT policy upon onboarding and whenever the policy is updated. Failure to acknowledge may result in restricted access to CAPIC systems.

9. Compliance and Legal Considerations

Regulatory Compliance

- **Compliance Guidelines:** Employees, including full-time and part-time employees, directors and volunteers, contractors, interns, consultants, must adhere to all relevant laws and regulations, such as GDPR, PIPEDA, and industry-specific requirements, to ensure compliance and avoid legal penalties.
- **Audits and Assessments:** Regular audits and assessments are conducted to ensure compliance with regulatory requirements and CAPIC's internal policies.

Data Privacy

- **Privacy Policies:** CAPIC's data privacy policies must be followed to protect personal and company data, ensuring confidentiality and proper handling of breaches and data loss incidents.
- **Breach Notification:** In the event of a data breach, CAPIC will notify affected parties as required by law and take steps to mitigate the breach.

10. Review and Updates

Regular Review

- **Policy Review Schedule:** The IT policy will be reviewed annually or more frequently if required by changes in the threat landscape, regulatory requirements, or business practices.
- **Policy Updates:** Updates to the policy will be communicated to all employees, who must acknowledge receipt and understanding of the changes.

Employee Feedback

- **Feedback Mechanism:** Employees are encouraged to provide feedback on the IT policy through designated feedback channels, such as surveys or direct communication with IT Governance team leader/ Manager.

- **Continuous Improvement:** Feedback will be reviewed regularly, and suggested improvements will be considered for future policy updates.

11. Personal Use and Privacy

Personal Device Use

- **Guidelines for Use:** Employees are allowed to use personal devices for work purposes only if they adhere to CAPIC's security standards, including installing approved security software and encrypting data.
- **Restrictions:** Personal devices may not be used to store sensitive company data. All work-related data must be stored on company-approved devices or secure cloud storage.

12. Privacy Expectations

- **Monitoring Policy:** CAPIC monitors work activities, including the use of IT resources, to ensure compliance with policies and protect company assets. Employees should have no expectation of privacy when using company resources.
- **Data Collection:** Monitoring data will be collected and stored securely, with access restricted to authorized personnel only.

13. Penalties for Non-Compliance

Consequences

a. **Disciplinary Actions:** Non-compliance with this IT policy may result in disciplinary actions including warnings, suspension, or termination of employment, depending on the severity of the violation.

b. **Legal Consequences:** Employees may also face legal consequences for breaches of confidentiality, data protection laws, or other regulatory requirements.

c. Third-party vendors may be subject to contract termination and legal action if they fail to adhere to this policy.

14. Onboarding Instructions

Pre-Arrival Preparation

a. **IT Account Setup:** Prior to the new employee's start date, the IT department will create user accounts, configure access permissions, and prepare devices.

b. **Equipment Provisioning:** Devices and necessary software will be pre-installed and configured for security compliance.

Day-One Onboarding

c. **Security Briefing:** New employees, including full-time and part-time employees, directors and volunteers, contractors, interns, consultants, will receive a security briefing that covers key policies, including device security, data handling, and incident reporting procedures.

d. **Access Provisioning:** Employees, including full-time and part-time employees, directors and volunteers, contractors, interns, consultants, will be provided with login credentials and guided through setting up multi-factor authentication (MFA) and other security measures.

Training and Resources

e. **Policy Training:** Employees, including full-time and part-time employees, directors and volunteers, contractors, interns, consultants, will undergo IT policy training to understand all security requirements, access controls, and acceptable use policies.

f. **Resource Access:** Employees, including full-time and part-time employees, directors and volunteers, contractors, interns, consultants, will be provided with access to all necessary resources, including the employee intranet, collaboration tools, and IT support contacts.

15. Securing CAPIC IT Property from Terminated or Absent Employees

Pre-Termination Procedures

a. **Notification and Planning:** HR will notify IT in advance of terminations or extended absences, and a risk assessment will be conducted to determine necessary security measures.

b. **Data Backup:** Data will be backed up or transferred to authorized personnel to prevent data loss.

Immediate Actions Upon Termination

c. **Account Deactivation:** All user accounts and remote access privileges will be immediately deactivated.

d. **Device Retrieval:** All company-issued devices will be collected, inspected, and securely wiped to remove all data.

Post-Termination Procedures

e. **Permanent Account Closure:** User accounts will be permanently deleted or archived as per policy requirements.

f. **Credential Changes:** All passwords and shared credentials accessible by the terminated employee will be changed.

Handling of Extended Absence

g. **Account Suspension:** Accounts will be temporarily suspended during extended absences, with access reinstated upon return.

h. **Device Security:** Devices not in use will be securely stored, and access rights will be reviewed and adjusted as necessary.

Communication and Documentation

i. **Communication Protocol:** Clear communication between HR, IT, and the employee's manager will be maintained to ensure proper procedures are followed.

j. **Documentation:** All actions taken during termination or absence will be documented in a termination checklist and incident report if necessary.

Legal and Compliance Considerations

k. **Legal Review:** All procedures will comply with relevant laws and CAPIC policies, ensuring legal and regulatory compliance.

l. **Data Retention and Privacy:** Data will be handled according to CAPIC's data retention policies respecting privacy rights.