Canadian Association of Professional Immigration Consultants

L'Association Canadienne des Conseillers Professionnels en Immigration

April 9, 2026, CAPIC–ACCPI™

Canadian Association of Professional Immigration Consultants

IT Governance and Risk Mitigation Policy

Originally Approved	December 3, 2024
Amended	April 2026
Classification	Internal
Authority	Board of Directors

Version	Date	Approved By
1.0	December 3, 2024	Board of Directors
1.1	April 9, 2026	Board of Directors

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, and equipment loss
- Outline procedures for responding to IT-related incidents effectively
- Ensure effective decision-making and value creation through the use of technology
- Establish governance standards for the IMMeSuite™ integrated digital platform and all member-facing technology services operated by CAPIC
- Ensure responsible deployment and oversight of artificial intelligence systems used both internally and in member-facing services

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.

Specific application to IMMeSuite™: This Policy applies to all ten IMMeSuite services — IMMeMentor, IMMeForum, IMMeFile, IMMeEducation, IMMeCentre, IMMeLegal, IMMeSupport, IMMeJobs, IMMeAffiliate, and IMMeMyConsultant — as well as the CAPIC Connect 2.0 dashboard, the MyConsultant.ca public directory, and the AI Annie intelligent assistant. All data collected, processed, stored, or transmitted through these platforms is subject to the provisions of this Policy and the CAPIC Privacy Policy.

Cross-border data handling: Where IMMeSuite services are accessed from outside Canada, CAPIC shall ensure that personal information transferred across borders is protected to a standard substantially similar to Canadian privacy law, in compliance with PIPEDA and applicable provincial legislation.

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 software 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:** All individuals within scope 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:** All individuals within scope 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.

2.2.1 Data Classification Framework

All data within CAPIC systems, including IMMeSuite services, shall be classified into the following categories:

- **Confidential:** Member personal information, financial data, client case files, disciplinary records, Board in-camera materials, and HR records. Access restricted to authorized personnel with a demonstrated need-to-know.

- **Internal:** Operational documents, internal communications, staff reports, policy drafts, committee materials, and IMMeForum moderated content. Access restricted to CAPIC staff, Directors, and authorized volunteers.
- **Public:** Published policy documents, MyConsultant.ca directory listings, marketing materials, and newsletters. No access restriction.

Data owners are responsible for classifying data within their service areas. A Data Classification Register shall be maintained and reviewed annually.

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:** All individuals within scope 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:** All individuals within scope 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 individual's role and need-to-know basis, ensuring access only to necessary information.
- **Role-Based Access Control (RBAC):** CAPIC utilizes RBAC to ensure that individuals 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 roles and responsibilities.

3.1 IMMeSuite Access Governance

Access to IMMeSuite administrative functions shall follow the principle of least privilege. Each IMMeSuite service area is responsible for managing user access within its scope. Member-facing access to IMMeSuite services is governed by CAPIC membership status; access is automatically suspended upon loss of membership in good standing, consistent with By-law 2024-1, s.2.8.

4. Use of Company Resources

Hardware and Software

- **Approved Use:** All individuals within scope 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:** Downloading or installing unauthorized software is prohibited to prevent malware and unauthorized software use. All software installations must be approved by IT.
- **Equipment Maintenance:** All individuals within scope are responsible for the proper use and maintenance of company-issued equipment and must report any issues or damages to the administrative coordinator immediately.

IT Support

- **IT Issue Reporting:** IT support is accessible 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, all individuals within scope must promptly contact the IT contractor. All issues should be reported to the IT Team to ensure efficient handling and timely resolution.

4.1 IT Procurement

All procurement of IT resources — including software licences, cloud services, SaaS subscriptions, hardware, and third-party vendor contracts — is subject to both this Policy and the CAPIC Procurement Policy. IT procurement must include a documented security assessment covering data handling practices, encryption standards, access controls, and compliance with PIPEDA.

5. Communication Tools and Protocols

Approved Tools

All work communications shall use CAPIC-approved communication and collaboration platforms. The approved tools list shall be maintained and reviewed annually. Approval of new communication tools shall require a documented assessment of security features, compliance with this Policy, and compatibility with existing CAPIC systems.

- **Tool Usage Guidelines:** All individuals within scope must follow usage guidelines for each approved tool, including proper setup, maintenance of communication channels, and adherence to security settings.
- IMMeForum is the designated platform for member-to-member professional discussions, per the CAPIC Communication Policy.

Communication Etiquette

- **Professional Conduct:** All individuals within scope must maintain professional conduct during all communications, adhering to CAPIC's guidelines for respectful and constructive communication.
- **Response Times:** All individuals within scope are expected to respond to work-related communications within established time frames, ensuring collaboration and productivity.

6. AI Usage Policy

6.1 Staff-Facing AI Usage

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 be used 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.

6.2 Member-Facing AI Systems (AI Annie)

CAPIC operates AI Annie, an intelligent in-platform assistant embedded across the IMMeSuite ecosystem. The following governance requirements apply to AI Annie and any future member-facing AI systems:

- **Transparency:** AI Annie must clearly identify itself as an AI assistant in all member interactions.
- **Accuracy and limitations:** AI Annie's outputs are informational and supportive. It shall not provide legal advice or render regulatory opinions. All outputs shall include appropriate disclaimers.
- **Data inputs:** Member data used by AI Annie is subject to the data classification framework and the CAPIC Privacy Policy.
- **Human oversight:** AI Annie's underlying models and behavioural guidelines shall be reviewed periodically. Material changes to its capabilities require appropriate authorization.
- **Ethical guardrails:** AI Annie shall not discriminate on the basis of any prohibited ground under the Canadian Human Rights Act and shall not be used to make or recommend decisions affecting member standing.
- **Audit trail:** Significant AI Annie interactions involving confidential data shall be logged and retained per the data retention schedule.

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 individuals within scope shall 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.

Expanded training requirements (March 2026):

- Frequency: Annual completion is required. New personnel must complete training within 30 days of commencing their role.
- Content scope: Data protection and PIPEDA obligations; device and network security; phishing awareness; incident reporting; AI usage guidelines; IMMeSuite platform-specific data handling; and the CAPIC Code of Conduct as it relates to information security.
- Compliance tracking: Training completion shall be tracked and reported regularly to ensure organizational compliance.
- Specialized training: Staff with administrative access to sensitive IMMeSuite services shall receive additional training on handling confidential member data, conducted at least annually.
- Directors and volunteers: Shall receive a condensed security awareness briefing at the beginning of each Board term or volunteer appointment.

Policy Acknowledgment

- **Acknowledgment Process:** All individuals within scope 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:** All individuals within scope 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 individuals within scope, 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 the IT Governance team.
- **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.

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.

12. Penalties for Non-Compliance

Consequences

- **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.
- **Legal Consequences:** Employees may also face legal consequences for breaches of confidentiality, data protection laws, or other regulatory requirements.
- Third-party vendors may be subject to contract termination and legal action if they fail to adhere to this policy.

13. Onboarding Instructions

Pre-Arrival Preparation

- **IT Account Setup:** Prior to the new employee's start date, the IT department will create user accounts, configure access permissions, and prepare devices.
- **Equipment Provisioning:** Devices and necessary software will be pre-installed and configured for security compliance.

Day-One Onboarding

- **Security Briefing:** New employees will receive a security briefing that covers key policies, including device security, data handling, and incident reporting procedures.
- **Access Provisioning:** Employees will be provided with login credentials and guided through setting up multi-factor authentication (MFA) and other security measures.

Training and Resources

- **Policy Training:** Employees will undergo IT policy training to understand all security requirements, access controls, and acceptable use policies.
- **Resource Access:** Employees will be provided with access to all necessary resources, including the employee intranet, collaboration tools, and IT support contacts.

14. Securing CAPIC IT Property from Terminated or Absent Employees

Pre-Termination Procedures

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

Immediate Actions Upon Termination

- **Account Deactivation:** All user accounts and remote access privileges will be immediately deactivated.
- **Device Retrieval:** All company-issued devices will be collected, inspected, and securely wiped to remove all data.

Post-Termination Procedures

- **Permanent Account Closure:** User accounts will be permanently deleted or archived as per policy requirements.
- **Credential Changes:** All passwords and shared credentials accessible by the terminated employee will be changed.

Handling of Extended Absence

- **Account Suspension:** Accounts will be temporarily suspended during extended absences, with access reinstated upon return.
- **Device Security:** Devices not in use will be securely stored, and access rights will be reviewed and adjusted as necessary.

Communication and Documentation

- **Communication Protocol:** Clear communication between HR, IT, and the employee's manager will be maintained to ensure proper procedures are followed.
- **Documentation:** All actions taken during termination or absence will be documented in a termination checklist and incident report if necessary.

Legal and Compliance Considerations

- **Legal Review:** All procedures will comply with relevant laws and CAPIC policies, ensuring legal and regulatory compliance.
- **Data Retention and Privacy:** Data will be handled according to CAPIC's data retention policies, respecting privacy rights.

15. Vendor and Third-Party Risk Management

All third-party vendors, service providers, and technology partners that access, process, store, or transmit CAPIC data are subject to the following requirements:

- **Vendor security assessment:** Prior to engagement, vendors must demonstrate compliance with CAPIC's data handling, encryption, and access control standards, as well as applicable Canadian privacy legislation.
- **Data processing agreements:** All vendors handling CAPIC member data must execute a written data processing agreement specifying permitted uses, security obligations, breach notification timelines, and data return or destruction upon termination.
- **Partner obligations:** Affinity programme partners that receive or access member data must comply with data protection standards set out in their respective agreements.
- **Ongoing monitoring:** Vendor compliance shall be reviewed on a regular basis. Material vendor security incidents must be reported and addressed promptly.

16. Incident Response

An IT security incident is any event that compromises or threatens the confidentiality, integrity, or availability of CAPIC IT systems, data, or services, including those supporting IMMeSuite. This includes unauthorized access, data breaches, malware infections, service outages, and AI system malfunctions.

- All suspected incidents shall be reported to the designated IT contact immediately.
- Incidents shall be assessed for severity and responded to promptly, with containment, investigation, and remediation steps documented.
- Significant incidents shall be followed by a post-incident review identifying root cause and informing policy improvements.
- Where a breach of personal information creates a real risk of significant harm, CAPIC shall fulfill its notification obligations under PIPEDA.

17. Business Continuity and Disaster Recovery

CAPIC shall maintain a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) for its IT infrastructure, including all IMMeSuite services. The BCP/DRP shall be reviewed and tested at least annually.

- **Data backup:** All CAPIC data shall be backed up regularly. Backups shall be encrypted, stored separately from primary systems, and tested for recoverability.
- **Recovery objectives:** Recovery time and recovery point objectives shall be established for each critical service, prioritized by member impact.
- **Communication plan:** The BCP shall include a communication plan for extended outages using channels independent of the affected systems.

- **Annual testing:** At least one recovery exercise shall be conducted annually, with results documented and used to improve the plan.

18. Governance Oversight and Accountability

- Oversight and Accountability: CAPIC maintains ongoing oversight of its IT governance framework to ensure security, compliance, and risk management practices are upheld across all systems, platforms, and services.
- Policy Alignment: This Policy shall be reviewed on a regular cycle and is read in conjunction with all related CAPIC policies, including the Privacy, Communication, Procurement, Conflict of Interest, and Code of Conduct and Ethics policies.

Approval

Approved by the Board of Directors of the Canadian Association of Professional Immigration Consultants (CAPIC–ACCPI).

Originally Approved	Amended
December 3, 2024	April 9, 2026

CAPIC–ACCPI™
Canadian Association of Professional Immigration Consultants
18 King Street East, Suite 1400, Toronto, ON, M5C 1C4 | (416) 483-7044 | www.capic.ca