

Global Information Security Policy

Commitment to Information Security

Manulife is committed to safeguarding the information, systems, and technology infrastructure that support our global operations through an enterprise-wide cybersecurity and technology risk program, supported by defined governance, clear accountability, and continuous improvement. Our program is informed by regulatory expectations and aligned to recognized industry standards.

We are committed to protecting customer and corporate data, maintaining secure and resilient systems, and enabling trusted business operations. We have clear policies that support our obligations to our customers, partners, and stakeholders through strong information security practices.

Governance & Cyber Risk Management

Manulife manages information and cyber risk through an enterprise-wide governance framework and enterprise-wide information security and cybersecurity program aligned to enterprise risk management practices. Oversight is provided by senior management and the Board, with defined roles responsible for setting risk appetite, allocating resources, and monitoring performance.

We apply a risk-based approach to identify, assess, and manage material risks arising from cybersecurity threats and evolving technologies across systems, applications, and third-party services. This approach is supported by a structured controls framework, with policies and standards establishing consistent expectations across the organization. Key risk indicators, control testing, and regular internal reporting support transparency and accountability.

Roles and responsibilities across the organization align with our three-lines-of-defense governance model, aimed at ensuring effective management, oversight, and independent assurance. Our framework is subject to ongoing review and enhancement to address evolving cybersecurity threats, emerging technologies, regulatory developments, and business needs. These processes support assessment of potential regulatory, supervisory, and disclosure obligations where required.

Cybersecurity Operations & Resilience

Manulife maintains a proactive cybersecurity program designed to detect, assess, and respond to threats. Continuous monitoring, vulnerability management, and threat intelligence capabilities support the timely identification and mitigation of risks.

We maintain defined incident response and escalation processes to manage security events and minimize impact. Our approach emphasizes operational resilience, including defined capabilities to recover effectively from disruptions. Response and recovery capabilities are periodically tested to ensure readiness and effectiveness.

Independent oversight and assurance functions regularly evaluate the effectiveness of controls and response capabilities.

Data Protection

Manulife protects data throughout its lifecycle to preserve confidentiality, integrity, and availability. We implement controls aligned to internal standards covering data classification, access management, encryption, secure application development, and records retention.

Manulife maintains dedicated privacy policies and practices to govern the collection, use, and protection of personal information, consistent with applicable regulations across the jurisdictions in which we operate. Data quality, accuracy, and appropriate use are reinforced through governance processes and ongoing monitoring.

Third-Party Risk Management

Manulife establishes clear information security expectations for third parties that process, store, or transmit Manulife information. Our approach includes risk-based due diligence, contractual requirements, and ongoing monitoring designed to ensure third parties maintain appropriate security safeguards, align with Manulife standards, and meet regulatory obligations, consistent with Manulife's risk management framework.

Third parties are subject to ongoing risk assessments to support effective oversight of associated risks.

Security Culture and Responsibilities

All employees and contractors are expected to uphold their responsibilities for protecting Manulife information and systems. We promote a strong security culture through training, awareness, and clear policies that define expected behaviors. Mandatory training programs support understanding of security obligations and emerging risks.

Employees are required to use approved systems, safeguard information, and promptly report security incidents or concerns. Roles and responsibilities across the organization support effective implementation, oversight, and independent challenge of security controls.

Our established information security program is a core component of Manulife's commitment to responsible governance, customer trust, and the protection of stakeholders in an increasingly interconnected and threat-prone environment.