# Information Security Policy

## 1. Introduction

Edge Factor is a Canada-based company that provides a Software-as-a-Service (SaaS) platform designed to help educators guide students on their career journey. The platform also enables employers and community organizations to highlight local training pathways and employment opportunities for learners and job seekers.

Edge Factor's platform is hosted entirely on **Microsoft Azure**, a cloud service provider known for its enterprise-grade security, scalability, and compliance. We do not operate or manage on-premise corporate infrastructure such as physical servers or private data centers.

Internally, Edge Factor uses third-party SaaS applications for operations (e.g., communications, file storage, CRM), all of which are carefully vetted to ensure alignment with our data privacy and security standards. No personal information is stored or processed on any self-hosted or unmanaged infrastructure.

## 2. Scope

This information security policy applies to all information processed and handled by Edge Factor, including data of customers and its own internal data.

This policy applies to **all Edge Factor personnel**, contractors, and third-party service providers who have access to our systems or data. It governs the **confidentiality, integrity, and availability** of information in accordance with applicable data protection laws and recognized industry standards (such as ISO/IEC 27001, SOC 2, and NIST SP 800-53).

## 3. Normative References

This information security policy is organized roughly according to ISO/IEC 27002:2022 (Information security cybersecurity, and privacy protection) information security controls.

## 4. Risk

Edge Factor conducts a formal **Information Security Risk Assessment** at least annually, or when significant changes occur in our systems, services, or threat landscape. This process identifies and evaluates risks to the confidentiality, integrity, and availability of data handled by the company.

The assessment considers both internal and external threats, including cybersecurity risks, operational vulnerabilities, regulatory changes, and data residency obligations. Risk levels are evaluated based on

**likelihood and impact**, and appropriate mitigation strategies are implemented based on industry best practices and business priorities.

Risk assessments are reviewed and approved by management, and their results are used to guide continuous improvement of our technical and organizational controls, consistent with ISO/IEC 27001, SOC 2, and NIST standards.

## 5. Goals

Edge Factor is committed to safeguarding the confidentiality, integrity and availability of all the information assets it owns or processes on behalf of its customers, in accordance with the risks, to ensure that regulatory, operational and contractual requirements are fulfilled.

## 6. Organization of Information Security

Edge Factor maintains a structured approach to information security management, with clearly defined responsibilities at all levels of the organization.

*Executive Responsibility*

The **Chief Technology Officer** holds overall accountability for information security at Edge Factor, including the security of personnel practices, IT systems, and customer data. The CTO is the designated owner of this Information Security Policy and is responsible for:

- Approving security standards, procedures, and access controls
- Ensuring secure system development and procurement practices
- Defining access rights for users and user groups based on roles and responsibilities
- Maintaining appropriate controls for internal and third-party services

*Staff Responsibilities*

All **employees, contractors, and consultants** are required to:

- Read, understand, and follow Edge Factor's Information Security Policy
- Ask questions or seek clarification from the CTO when unsure about data handling responsibilities
- Report any security concerns, suspected incidents, or policy violations promptly

*Use of Devices*

- Use of **mobile or personal devices** for work must be explicitly approved by management.
- Employees must notify their manager **before** accessing company or user data on a new or personal device to ensure proper security controls are in place (e.g., encryption, remote wipe, password protection).
- Edge Factor reserves the right to enforce additional rules regarding device security.

*Remote Work*

Working remotely is permitted with management approval. Since Edge Factor operates primarily through cloud-based systems and does not rely on internal office servers to process or store user data, **remote**

**work is treated as functionally equivalent** to in-office operations from a security perspective. All applicable security policies apply regardless of work location.

## 7. Human Resource Security

*7.1 Prior to Employment or Engagement*

A. All employees, contractors, and third-party personnel who may access sensitive or internal information must sign a **confidentiality agreement**, typically included in standard employment contracts or vendor agreements.

B. All relevant individuals will receive and acknowledge this **Information Security Policy** and the company's **Privacy Policy** as part of onboarding. These obligations extend to consultants, vendors, and third parties who require access to company systems or data.

*7.2 During Employment*

A. All users must adhere to the information security requirements outlined in this document and in all supporting policies.

B. Edge Factor requires all employees and authorized third parties to **review the Information Security and Privacy Policies at least once annually**, or when material changes occur.

C. **Annual training** is mandatory for all staff, covering key topics such as secure data handling, privacy expectations, and incident reporting procedures. Refresher training is also required following significant policy updates.

D. Violations of these policies may result in disciplinary action in accordance with HR procedures.

E. Company information, systems, and equipment may only be used for authorized business purposes. Limited personal use of company-issued devices is permitted, provided it does not involve external commercial activity or compromise information security.

*7.3 Termination and Change of Employment*

A. Upon **termination or change of role**, user access rights will be updated or revoked without undue delay.

B. Exit procedures include revoking system credentials, collecting company devices (if any), and reminding personnel of continuing confidentiality obligations.

## 8. Asset Management

Edge Factor takes care to manage its information and IT assets responsibly and securely throughout their lifecycle—from acquisition to disposal. This ensures the confidentiality, integrity, and availability of systems and data.

*8.1 Inventory and Ownership*

A. Edge Factor maintains a centralized **inventory of information and IT assets**, including hardware, software, cloud accounts, and data repositories.

B. Each asset is assigned an **owner** who is responsible for ensuring it is used and maintained according to company policy.

*8.2 Acceptable Use and Responsibility*

A. All employees, contractors, and third-party users must adhere to Edge Factor's **Code of Conduct for Security and Privacy**, which outlines acceptable use of company-owned IT assets.
B. Any use of company assets must align with Edge Factor's business objectives and must not compromise the security of information or systems.
C. The use of unauthorized software or hardware on Edge Factor systems is strictly prohibited without explicit approval from management.

*8.3 Asset Return and Disposal*

A. All company-issued equipment (e.g., laptops, mobile devices, accessories) must be **returned upon termination of employment**, end of contract, or when no longer needed.
B. Returned devices are securely wiped before reassignment or disposal, following Edge Factor's data sanitization standards.
C. Any disposal of physical or digital assets is conducted in accordance with applicable privacy and data protection regulations (e.g., PIPEDA, GDPR, CCPA).

## 9. Access Control

Edge Factor enforces strict access control measures to protect the confidentiality, integrity, and availability of its systems and the data it processes. Access is granted based on business needs, job responsibilities, and compliance with security best practices.

*9.1 Business Requirements for Access Control*

A. Access control and password management policies are defined in writing and regularly reviewed to ensure alignment with current **security risks and operational needs**.
B. All users must be **authenticated** before accessing company systems. Authentication methods include strong passwords and multi-factor authentication (MFA) where applicable.
C. The **principle of least privilege** is applied to ensure users are only granted the minimum access necessary to perform their duties.
D. When roles change or employment ends, access rights are reviewed and adjusted accordingly.

*9.2 User Access Management*

A. All system access is authorized and managed by the **Operations team** based on defined user roles and access requirements.
B. **Access to high-risk or sensitive systems** is subject to periodic review to detect and revoke unnecessary access privileges.
C. Temporary or administrative access is time-bound and logged.

*9.3 User Responsibilities*

A. Each user is provided with a **unique email and login credential** upon onboarding.

B. Users are responsible for the **confidentiality and security** of their credentials and must not share passwords.
C. Users must immediately change the system-generated password to a strong, unique one upon first login.
D. Employees are encouraged to use a **company-approved password manager** to store and generate passwords securely.
E. All devices used for work must be secured with **strong passwords or biometric authentication**.
F. User-generated passwords must meet minimum complexity standards:
   - Minimum 8 characters
   - At least one uppercase letter
   - At least one special character (e.g., !@#$%^&*)
   - No common or dictionary words

G. **Multi-Factor Authentication (MFA)** is mandatory for:
   - Google Workspace (enforced using Google Authenticator)
   - Any third-party service supporting MFA (e.g., GitHub, Azure, AWS)

*9.4 System and Application Access Control*

A. Access control is **enforced automatically** by systems based on the user's role or group membership.
B. Elevated or administrative privileges are limited to **authorized personnel only**, with additional security requirements (e.g., MFA, logging).
C. Access to **source code repositories** is strictly controlled.
D. Access to **staging and production environments** is limited to approved engineers and system administrators. All access is logged and reviewed.

## 10. Cryptography

Edge Factor applies strong cryptographic controls to safeguard Personal Data and authentication credentials, in accordance with industry standards and regulatory requirements across Canada, the U.S., and the EU.

*10.1 Encryption of Customer Data*

A. **Encryption at Rest**: All customer data stored in Azure infrastructure (including SQL Server databases) is protected using Azure's built-in **Transparent Data Encryption** and **Storage Service Encryption** features, as applicable.
B. **Encryption in Transit**: All communications and data exchanges between users and Edge Factor services are protected using **TLS 1.2 or higher**. SSL certificates are issued by trusted Certificate Authorities (e.g., Let's Encrypt) and renewed automatically.
C. **Key Management**: Edge Factor uses **Azure-managed keys** for encryption by default. When applicable, support for **Customer-Managed Keys** is available to enterprise clients upon request.

*10.2 Endpoint Encryption*

A. All laptops issued to employees, contractors, and consultants must have **full-disk encryption** enabled using platform-native tools:
   - macOS: **Apple FileVault 2**
   - **Windows: BitLocker Drive Encryption**

B. **Recovery keys** must be stored securely using a company-approved key management solution accessible only by authorized IT administrators.

*10.3 Cryptography*

Edge Factor follows **conservative cryptographic practices** for all use cases not covered by default platform protections.

## 11. Physical and Environmental Security

*11.1 Secure Areas*

A. Edge Factor does not host or store customer data in any on-premise systems or office-based infrastructure. All systems and customer data are hosted securely within **Microsoft Azure**, which maintains robust, independently verified certifications, including:
   - **ISO 27001**, **ISO 27017**, **ISO 27018**
   - **SOC 1, SOC 2, SOC 3**
   - **PCI-DSS, CSA STAR, and more**
   - **Detailed compliance documentation is available at: Azure Compliance Offerings.**

B. Edge Factor's office space is leased within a multi-tenant commercial facility. **Physical access control and surveillance** are the responsibility of the property manager and are administered in accordance with Edge Factor's security guidelines. No internal office networks or on-premise servers are used to host customer data or production systems.

*11.2 Equipment and Workstation Security*

A. Customer data or other **sensitive information** must not be stored on portable media (e.g., USB drives, external HDDs, mobile phones) unless **absolutely necessary** and pre-approved by management. In such cases, data must be **fully encrypted** and **password protected** using approved tools.

B. Company laptops and devices must remain in the custody of the employee when travelling and treated as **carry-on luggage** whenever possible.

C. **Automatic screen lock** must activate after **no more than 3 minutes of user inactivity**, and devices must not be left unattended while logged in or unlocked.

D. Printed materials containing Personal Data must be:
   - Stored in a **locked cabinet** approved by the CTO.
   - **Shredded or securely destroyed** when no longer required for operational or legal purposes.

E. Lost or stolen devices must be **reported to management immediately**. Devices should have full disk encryption and remote wipe capabilities enabled where applicable.

F. Before disposal of electronic equipment, all Personal Data must be securely **erased using industry-standard data destruction tools** that render recovery infeasible (e.g., cryptographic wiping or certified hardware destruction services).

## 12. Operations Security

A. All updates and deployments to the Edge Factor platform must be **centrally logged** using secure logging infrastructure. Logs must be **tamper-evident** and protected against unauthorized access, deletion, or modification.

B. **System logs relevant to security and platform health** shall be reviewed regularly to detect anomalies, ensure platform reliability, and support incident response procedures.

C. All systems and endpoints exposed to malware risk (e.g., employee workstations, admin consoles, or web servers) must have **up-to-date malware and antivirus protection** in place, with **real-time scanning and automatic updates** enabled.

D. Server patching policy:

- **Critical security patches** must be applied within **24 hours** of release.
- **General updates and non-critical patches** must be applied within **two weeks** of release.
- Automated tools and monitoring systems should be used to enforce this policy and alert on deviations.

E. **Employee workstation updates**: All staff must install security updates on company-managed devices **immediately upon availability** or allow automatic system updates where applicable.

F. **Backup Policy**:

- Backups must be performed according to a **documented and tested backup schedule**, aligned with Edge Factor's **Recovery Point Objective** and **Recovery Time Objective**.
- Backups must be **encrypted**, **stored securely**, and tested **regularly** to ensure data restoration integrity.

G. **Security audits and penetration testing** must be **strategically planned and executed** to minimize any impact on production systems. When possible, audits should be scheduled during low-traffic periods and carried out in isolated staging environments.

## 13. Communications Security

A. For all systems in the Azure environment, appropriate firewall rules (security groups) are configured.

B. Electronic messaging is outsourced to Google G-Suite, SendGrid, and Signal One which provides adequate safeguards for the security of emails.

## 14. System Acquisition, Development, and Maintenance

*14.1 Security Requirements for Information Systems*

A. Security and privacy requirements must be embedded into the **design, development, and maintenance** of all new systems and features.

B. Edge Factor applies **Privacy by Design and Privacy by Default** principles in every phase of the system lifecycle to ensure compliance with applicable data protection laws.

C. Functional and non-functional security controls, such as **authentication, authorization, audit logging, input validation, and encryption**, are specified at the start of every development project.

*14.2 Security in Development and Support Processes*

A. All code developed by Edge Factor is stored in **Azure DevOps** with full version control and access restrictions.
B. All software changes follow a structured release pipeline: **Development** → **Staging** → **Production**, with automated and manual testing at each phase.
C. **Peer code reviews** are mandatory for all changes, with a focus on identifying vulnerabilities and maintaining secure coding practices.
D. Developers receive ongoing **secure coding training**, and are expected to follow modern security practices.
E. In urgent or emergency situations, a fast-tracked deployment may be approved. In such cases, post-deployment **retrospective testing and documentation** are required to maintain audit readiness and accountability.
F. All deployed applications and system configurations must be **hardened** based on current industry best practices (e.g., Center for Internet Security Benchmarks).

*14.3 Test Data*

A. The use of **real customer data in development or testing environments is strictly prohibited**.
B. Only **anonymized or synthetic test data** may be used in local development environments or shared testing environments.
C. Any exception to this rule must be documented, justified, approved by the CTO, and protected with the same controls as production data.

## 15. Supplier Relationships

A. **Risk-Based Due Diligence:** Prior to onboarding any third-party service provider that will process, store, or transmit data (especially when the data falls under **high or medium security classifications**) Edge Factor will conduct risk-based due diligence. This evaluation may include:
   - Reviewing publicly available information,
   - Verifying third-party **security certifications** (e.g., ISO 27001, SOC 2, CSA STAR),
   - Confirming adherence to recognized **Codes of Conduct** or Frameworks (e.g., NIST),
   - Requesting and reviewing **audit reports**,
   - Holding direct security review meetings with the vendor.

B. **Ongoing Assurance:** For any third-party vendors processing personal or sensitive data with elevated security requirements, **annual reviews** of their security certifications, audit results, and privacy compliance posture shall be conducted to ensure continued adequacy.
C. **Data Processing Agreements (DPAs):** A formal **Data Processing Agreement** must be in place with every third-party supplier or sub-processor that receives, stores, or otherwise accesses Personal Data on Edge Factor's behalf. These agreements must define:
   - Roles and responsibilities,

    - Permitted processing activities,
    - Security controls,
    - Incident reporting procedures,
    - Geographic data transfer protections (e.g., Standard Contractual Clauses).

D. **Right to Audit Clause:** Contracts with suppliers handling personal data should contain a **right to audit clause** allowing Edge Factor to assess the supplier's compliance with relevant security and privacy obligations, if needed.

E. **Data Minimization Principle:** Suppliers should only be granted access to the minimum amount of data necessary for them to fulfill their service obligations.

## 16. Information Security Incident Management

A. **Definition of an Incident:** Any breach, suspected breach, or deviation from standard operating procedures that compromises, or could potentially compromise, the confidentiality, integrity, or availability of Edge Factor's information systems or Personal Data shall be classified as an **information security incident**.

B. **Employee Responsibilities:** All employees, contractors, and relevant third parties are required to **immediately report** any suspected or actual information security incident. Reports must be made to both the **Chief Technology Officer** and the **Privacy Officer** without delay.

C. **Incident Reporting Process:** A documented **Incident Response Procedure** shall be maintained, which outlines:
    - How to identify and categorize incidents,
    - Reporting lines and timelines,
    - Roles and responsibilities during incident handling,
    - Communication protocols (internal and external),
    - Documentation and root cause analysis steps.

D. **Personal Data Breach Response:** In accordance with legal and contractual obligations (including under **GDPR Article 33**, **PIPEDA**, **MFIPPA**, and **CCPA/CPRA**), the procedure shall include guidelines for:
    - Notifying affected customers and individuals without undue delay when required,
    - Coordinating with regulatory authorities (e.g., the Office of the Privacy Commissioner of Canada, supervisory authorities in the EU, or California Attorney General),
    - Maintaining incident logs and evidence for audit or legal purposes.

E. **Post-Incident Review:** After each incident, a formal **post-incident review** must be conducted to:
    - Identify root causes,
    - Implement remediation and preventative controls,
    - Update procedures or policies if needed.

F. **Testing and Training:** The incident management plan shall be tested **annually**. All employees must receive training on incident recognition and response protocols as part of their ongoing security awareness program.

## 17. Business Continuity and Disaster Recovery Management

A. **Business Continuity Objective:** Edge Factor is committed to maintaining the availability of its services and the integrity of customer data during and after unexpected disruptions. Business continuity and disaster recovery (BC/DR) capabilities are in place to ensure minimal operational downtime and rapid recovery of services.

B. **Disaster Recovery Plan:** A documented **Disaster Recovery Plan** shall be maintained, outlining the procedures to recover data and restore critical systems in the event of a disaster or major system failure. The plan includes:
   - Roles and responsibilities,
   - Communication strategies,
   - Recovery steps for systems and data,
   - External contact protocols (e.g., regulators, customers).

C. **Plan Ownership and Execution:** The **Chief Technology Officer** holds responsibility for coordinating and overseeing all recovery operations during a disaster event.

D. **Redundancy and Resilience**:
   - All critical application and storage services operated by Edge Factor are deployed in **redundant configurations across at least two Azure Availability Zones**, ensuring high availability and geographic resilience.
   - Application servers are **stateless** and do not store user data; all user data is managed centrally in secured storage systems.

E. **Backup Strategy**:
   - **Daily backups** of customer data are performed and stored securely in a **separate Azure Region** from the primary data location.
   - Backups are encrypted and monitored continuously to ensure successful execution and integrity.
   - **Retention periods** and **backup schedules** align with regulatory and contractual requirements.

F. **Testing and Evaluation**:
   - The Disaster Recovery Plan shall be **reviewed and tested at least annually** to ensure operational effectiveness and up-to-date procedures.
   - A **full restore test of the production environment** must be conducted **at minimum every six (6) months** to validate data recovery capabilities and identify potential gaps.

G. **Continuous Improvement:** Lessons learned from tests or actual incidents are incorporated into updated business continuity plans and technical safeguards.

## 18. Compliance

A. **Regulatory and Legal Compliance:** Edge Factor ensures that all applicable **legal, regulatory, and contractual obligations** related to information security, privacy, and data protection are identified, tracked, and adhered to. This includes but is not limited to:
   - **ISO/IEC 27001:2013** (Information Security Management),
   - **SOC 2** (System and Organization Controls),

- **NIST Cybersecurity Framework**,
- **PIPEDA** (Canada),
- **MFIPPA** (Ontario education sector),
- **GDPR** (EU),
- **FERPA and CCPA** (U.S. education and consumer privacy laws).

B. **Penetration Testing & Security Audits:** To ensure the effectiveness of its security controls, Edge Factor conducts an **annual penetration test and/or third-party security audit** of its high-risk systems. Currently, testing is performed using tools and services and the results are reviewed and addressed promptly by the technical leadership team.

C. **Vendor Compliance:** Third-party service providers and subprocessors are evaluated for compliance with equivalent data protection and security standards. Where required, **Data Processing Agreements (DPAs)** are in place.

D. **Policy Review:** This Information Security Policy and associated procedures are reviewed **at least annually** and updated as necessary to reflect changes in business practices, technology, or regulatory requirements.