Information Security Policy

1. Introduction

Edge Factor is a company based in Canada which offers a platform in the form of Software as a Service (SaaS) that enables educators to guide and speak into their students' career journey. It also allows companies and community leaders to showcase career and training opportunities to local users in their community.

The Service runs entirely off of Microsoft Azure. For its corporate systems, Edge Factor makes use of SaaS offerings from many different vendors. Edge Factor does not own any corporate IT (servers, network) infrastructure that collects personal information.

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.

3. Normative references

This information security policy is organized roughly according to ISO/IEC 27002:2013: Information technology - Security techniques - Code of practice for information security controls.

4. Risks

The company should perform a risk assessment annually, in order to ensure that the security measures are still adequate to cover the risks.

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

1. The CTO has the overall responsibility for information security, including information security regarding personnel and IT security. The CTO is the owner of the security policy (this document).The CTO is responsible for purchasing requirements, development and maintenance of information and related information systems. The CTO must define which users or user groups are allowed access to the information and what authorized use of this information consists of.
2. Employees, contractors and consultants are responsible for getting acquainted with and complying with Edge Factor's information security policy. Questions regarding the administration of various types of information should be posed to the CTO.
3. Employees, contractors and consultants are allowed to use mobile devices to perform their work only with permission from management. The company can set specific rules regarding the use of mobile devices.
4. You must inform your manager before accessing data on a new or personal device. This allows us to ensure that the device is secured properly and that personal data is securely disposed of.
5. Working remotely is allowed with permission from management. Edge Factor does not use an internal IT system to collect, store, process, or distribute user information on the office network; therefore working remotely is effectively equivalent to working from the Edge Factor offices.

7. Human resource security

7.1 Prior to employment

1. A confidentiality agreement should be signed by employees, contractors or others who may gain access to sensitive and/or internal information. For employees this is included in their employment contract.
2. This information security policy and privacy policy should be provided and accepted as part of all employment contracts, and to contractors, consultants and other third parties if they need system access.

7.2 During employment

1. All users must comply with the information security requirements described in this document.

2. The information security policy and relevant supporting documentation should be reviewed annually by all employees.
3. All employees and third party users should receive adequate training regarding the information security policy, privacy policy, and procedures at least annually, and when major changes are made to the policies and procedures.
4. Breaches of the information security policies and procedures by employees can lead to HR sanctions.
5. Edge Factor's information, information systems and other assets must only be used for their intended business purposes. Necessary private use of personal computing devices issued by the company is permitted, except for commercial use outside of the scope of the company.

7.3. Termination and change of employment

1. Edge Factor will change or terminate access rights accordingly at termination or change of employment.

8. Asset management

1. Management maintains an inventory of information and IT assets operated by the company.
2. Company assets (e.g. laptop, mobile phone, etc) should be returned to the company at the conclusion of the need for the use of these assets.
3. All employees must agree to the Code of Conduct for Security and Privacy, which lays out the acceptable use of IT assets.

9. Access control

9.1 Business requirements

1. Written guidelines for access control and passwords based on business and security requirements should be in place. Guidelines should be re-evaluated on a regular basis.
2. Users accessing systems must be authenticated according to guidelines.
3. The principle of least privilege is applied for access to Edge Factor's information. New employees, or employees changing roles will be assessed for the access they need in order to perform their job.

9.2 User access management

1. Access to information systems should be authorized and/or implemented by the Operations team, on a "need to know" basis, regulated by the user's role in the company.
2. Periodic review should be performed for high-risk accounts to detect and prevent unauthorized employees who may still have access.

9.3 User responsibilities

1. Users are assigned a unique email address when they start to work for Edge Factor and a temporary initial password.
2. Users are responsible for any usage of their company accounts and passwords.
3. Users should keep their passwords confidential and not disclose them.
4. Employees must change their password to one of their own choice immediately.
5. Employees may use a company-approved password manager with automatically generated, unique passwords for all work-related accounts that are not the Computer Password or the Password Manager credentials.
6. All devices used by employees must be password protected.
7. User-chosen passwords must comply with the following complexity requirements:
    a. 8 characters minimum
    b. At least one capital letter
    c. At least one special character (e.g. !@#$%^&*(){}[])
    d. No dictionary words
8. All employees must use 2-Step Verification using Google Authenticator to access Google GSuite (e.g. Edge Factor Email). This must be enforced on the company level.
9. For any other service the company uses that offers two factor authentication, it is required to enable it (e.g. Github, Azure).

9.4 System and application access control

1. Applications and systems should automatically enforce access controls based on the user's privilege level.
2. Access to privileged accounts and sensitive areas should be restricted.
3. Only authorized employees can have access to Edge Factor's source code repositories.

4. Source code must not be publicly shared unless authorized by management, or when the source code has been released under Edge Factor's open-source program.
5. Only authorized employees are allowed access to staging and production systems.

10. Cryptography

Where technically possible, all personal data as well as authentication data should be appropriately protected by encryption and/or cryptographic hashing. In the case of customer data:

- For encryption at rest, Azure/SQL Server built-in encryption features should be enabled
- For encryption in transit, always use TLS encryption (LetsEncrypt)

For any specific use cases not covered by the above, the following document should be used as a guideline: http://latacora.singles/2018/04/03/cryptographic-right-answers.html

All laptops used by Edge Factor employees and contractors should be encrypted using the built-in disk encryption software (Apple FileVault 2 or BitLocker), and the company should retain the recovery keys in a safe location.

11. Physical and environmental security

11.1 Secure areas

1. Edge Factor does not have systems with (customer) data at office locations. All infrastructure is outsourced to Azure, a professional organization with multiple security certifications and third-party reports such as ISO 27001, ISO 27017, ISO 27018, SOC1, SOC2, SOC3, PCI-DSS, etc. More info about Azure compliance is available at https://docs.microsoft.com/en-us/azure/compliance/.
2. Edge Factor offices are located in an office space, operated by a commercial landlord. The office space provider is responsible for enforcing access controls (based on instructions by Edge Factor) and camera systems. Edge Factor does not operate internal IT systems hosted in any private office network in its offices.

11.2 Equipment

1. Information classified as "sensitive" (e.g. customer data) should not be stored on portable data carriers (e.g. laptops, cell phones, memory sticks, USB hard drives etc.).

If it is absolutely necessary to store this information on portable equipment, the information must be password protected and encrypted.

2. During travel, portable computer equipment should be treated as carry-on luggage.
3. Password protected screen savers should be enabled and should protect the computer within 5 minutes of user inactivity. Computers should not be unattended with the user logged on and no password protected screen saver active. Users should not leave their computers unlocked.
4. Any print materials that contain Personal Information must be stored in a locked cabinet that is approved by the CTO. These materials and documents must be shredded and properly disposed of when they are no longer required for operational purposes.
5. Employees must report all lost or stolen devices to management immediately.
6. Personal Data must be securely destroyed before obsolete electronic equipment is disposed of.

12. Operations security

1. All updates that are pushed to the Edge Factor platform must be logged centrally, and the logs protected from deletion and modification.
2. Relevant logs should be reviewed regularly to ensure proper working of the systems.
3. All systems that are typically susceptible to malware should have adequate malware protection installed.
4. All servers should be kept up-to-date with the latest security updates within two weeks of patches being released, except for emergency patches, which should be deployed within 24 hours.
5. Employees should install security updates on their company computers as soon as they become available.
6. Backups should be taken according to a predefined schedule in accordance with the company's recovery point objective and recovery time objective.
7. Audits should be appropriately planned in order to minimize disruption to the production systems.

13. Communications security

1. For all systems in the Azure environment, appropriate firewall rules (security groups) are configured.
2. 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

1. When building new systems or making changes to existing systems, security requirements and considerations must be an integral part of the process.
2. All software developed by Edge Factor must comply with the Privacy by Design and Privacy by Default philosophies.

14.2 Security in development and support processes

1. All application code must be stored in source control (Azure DevOps).
2. All software changes must go through the regular change process: via development, then staging, then to production.
3. Code reviews should be performed to keep the source code quality high and minimize the risk of security issues.
4. Developers should be trained on the principles of secure coding and apply those principles to the Edge Factor platform.
5. In case of emergency changes, some steps of the change process can be bypassed temporarily. Testing procedure and formal acceptance should then be performed retrospectively.
6. Applications and infrastructure configurations must be appropriately hardened according to industry best practices.

14.3 Test data

1. It is not allowed to use privacy sensitive customer data in a local development environment.

15. Supplier relationships

1. Before engaging a new service provider that will process information for which high or medium security requirements are necessary, due diligence should be performed in

order to assess whether the service provider is able to adequately protect the data. Due diligence can be performed by researching public information, verifying security certifications or codes of conduct, performing an audit, or by engaging in a conversation with the service provider.

2. For service providers that process information for which high security requirements are necessary, their security certifications should be reviewed annually.
3. Edge Factor should have a Data Processing Agreement with all third parties it exchanges personal data with.

16. Information security incident management

1. All breaches of security, including the use of information systems contrary to operating procedure, should be treated as incidents.
2. All employees are responsible for reporting (possible) breaches of security. Incidents should be directly reported to the CTO and the Privacy Officer. A procedure should be available detailing how to handle breaches of personal data, including the legal and contractual notification requirements.

17. Business continuity management

1. A disaster recovery plan must be developed and documented which contains a process enabling Edge Factor to restore any loss of data in the event of a system failure.
2. In the situation of a disaster, Edge Factor's CTO will be in charge of the recovery operation.
3. The disaster and recovery plan should be evaluated and tested annually.
4. Every software service operated by Edge Factor should run redundantly in two separate Azure zones. This applies for both application and storage services.
5. Application servers should not contain any user data. User data should always be stored within the storage system.
6. Every day a backup should be made of the customer data. The backups should (also) be stored in a different Azure Region than the original data.
7. Backup performance must be monitored to ensure backups are made successfully.

8. Every 6 months a full restore test of the production environment should be performed.

18. Compliance

1. All legal and contractual requirements should be identified and complied with.
2. The security of Edge Factor's high risk systems should be tested annually by means of a penetration test or security audit, currently performed by Acunetix.