FRAXION

Incident response plan

Cyber security incident response plan

T: 206-256-0771

1000 Second Avenue
Suite 2500
Seattle, WA 98104

info@fraxion.biz
fraxion.biz

Cyber security incident response plan

The purpose of this document is to manage and mitigate cyber security incidents efficiently, minimizing impact on services and ensuring continuity and integrity of operations and data. This plan covers all software services, databases, and support systems hosted on Microsoft Azure used by the company, its employees, and its customers.

Risk mitigation

Multi-factor authentication (MFA): We prioritize the security of our systems and data. As part of our commitment to safeguarding our assets, we use of Multi-Factor Authentication (MFA) to enhance security credentials and protect against unauthorized access.

Role-based access control (RBAC): We implement robust access controls to ensure that the right individuals have the appropriate access to resources, thereby minimizing the potential for abuse.

Encryption: We ensure that data is encrypted both in transit and at rest, utilizing strong cryptographic methods. We use tools such as Azure Key Vault to manage cryptographic keys securely and effectively.

Threat detection and response: We use Azure Security Center, which provides advanced threat protection mechanisms and security management tools. These tools are used to detect, analyze, and respond to potential threats, ensuring the security of our systems and data.

Data resilience: Azure ensures data durability and availability through redundant storage and robust backup solutions to prevent data loss even in the event of hardware failure. We have zone-redundant, read-only backups in place for all production databases. Additionally, we maintain up to 31 days of point-in-time restore backups and 12 months of weekly backups.

Regular audits and updates: We implement continuous monitoring and regular updates to our services and infrastructure. This proactive approach helps protect against vulnerabilities and ensures the security of our systems.

Roles and responsibilities

Each team member is responsible for initiating, managing, and closing incidents as per their role definition.

- Chief Information Officer (Marius Croucamp): Oversees the integrity of enterprise information and data security, shapes the organization's security strategy, manages risks, and ensures regulatory compliance.

- Incident Response Manager (Blair O'Neill): Leads the team, coordinates the response actions, and communicates with upper management and stakeholders.
- Security Analysts (Byron Theunissen): Responsible for initial analysis, monitoring security systems, and conducting detailed follow-up investigations to understand the scope and impact of the incident.
- Network Engineer (Stephen Desmore): Focus on maintaining secure network operations and managing changes to network infrastructure to isolate affected systems.
- IT Manager (Imraan Abderoef) - Oversees the selection, deployment, and management of cybersecurity tools and technologies, such as firewalls, antivirus software, intrusion detection systems, and encryption protocols.

Identification of incidents

We have implemented robust cybersecurity measures including the use of Azure security monitoring tools to detect anomalies and maintain comprehensive incident logs. This approach ensures that all detected incidents are thoroughly documented, including details of the actions taken and resolutions achieved.

Classification and prioritization

We classify cybersecurity incidents based on their impact and complexity, categorizing them into levels such as Critical, High, Medium, and Low to prioritize response efforts effectively. When prioritizing incidents in cybersecurity, our focus is on giving the highest priority to those that impact critical services. The SLA hours for each category are as follows:

Critical: 1 hour

High: 4 hours

Medium: 12 hours

Low: 24 hours

Response procedures

Initial response: When a security incident occurs, we first assess and determine how serious it is, then we work to contain it to prevent any additional harm, and immediately alert our Incident Response Team to handle the situation.

Investigation: We investigate by collecting and preserving evidence to understand what caused the incident and how extensive it is.

Eradication and recovery: We eradicate the root cause of the incident and then plan and implement the recovery of affected systems.

Post-incident review: We analyze the effectiveness of our response and update the Cyber Security Incident Response Plan as needed, while also documenting findings and lessons learned in the incident log.

Software security measures

Software security models such as OWASP SAMM outline the desired security posture of our framework. Security testing is carried out utilizing Burp Suite, with focused security assessments conducted in Development and Project environments, and thorough security scans performed in Test and Production environments with each major release. We adhere to secure coding practices and conduct peer reviews to uphold code quality, standards, and security best practices. OWASP serves as a guideline for the security risks engineers should remain mindful of. For infrastructure security, Azure Front Door manages routing and firewall security. Fraxion utilizes Azure's managed firewall rule sets, currently implementing the latest ruleset, DRS 2.1 Azure Web Application Firewall DRS rule groups and rules.

We collaborate with third-party security firms that conduct regular penetration tests on our products. Our security posture certificate can be made available upon request.

Communication

Internal communication: Notify all stakeholders and brief them on the situation, actions taken, and status updates.

External communication: Manage communications with customers through the Incident Response Manager (Blair O'Neill).

Training and awareness

Fraxion has implemented cybersecurity training and awareness programs that educate employees on the importance of cybersecurity, best practices for protecting sensitive information, and how to recognize and respond to security threats. These programs cover topics such as password security, phishing awareness, data protection, and the secure use of company systems and devices. Regular training sessions and simulated exercises ensure that employees are well-prepared to protect against cyber threats and respond effectively in the event of an incident. We conduct weekly security team catch-ups with the Cyber Security Response Team.

Documentation and record keeping

We maintain detailed records of all security incidents, including incident reports, logs, and communications in Confluence for future reference, compliance, and audit purposes.

Review and maintenance

We regularly review and update the Cyber Security Incident Response Plan (CSIRP) based on new threats, technological changes, and lessons learned from past incidents. Additionally, we audit and update our incident response tools and procedures to ensure they remain effective and up to date. Furthermore, we conduct monthly meetings with our Cloud Solution Architect at Microsoft to enhance our cloud computing platform.