FORESIGHT

PEOPLE BUILD FASTER WITH AI

WHITEPAPER

FORESIGHT CYBER SECURITY STRATEGY

EXECUTIVE SUMMARY

1 Introduction

Foresight is a leading AI SaaS platform designed specifically for megaproject management. Foresight, efficiently processes and analyses vast amounts of schedule data from megaprojects, extracting critical information and transforming raw data into actionable insights. By leveraging Foresight's advanced capabilities, project teams can streamline their operations, ensure timely project delivery, and smoother project management experience.

Foresight works by ingesting schedule files from existing systems such as Primavera P6 and Microsoft Project. Foresight is a fully cloud based solution, available in browser, and requiring no integration with any other IT system or infrastructure.

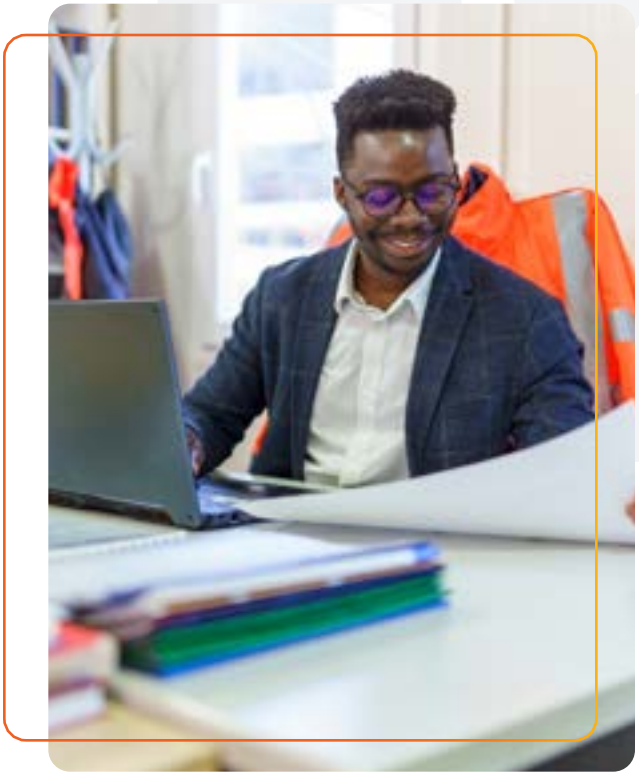
Selection of customers who have granted IT & Cybersecurity clearance to Foresight:

Government Agencies & Public Bodies:

- Ministry of Defence (UK)
- Nuclear Decommissioning Authority (UK)
- Atomic Energy Authority (UK)
- Metrolinx (Canada)
- National Transport Administration (Israel)
- Ministry of Health (New Zealand)
- Crossrail Ltd (UK)

Critical Infrastructure Owners & Developers:

- Chevron (USA)
- Microsoft (USA)
- Alstom Transportation (USA)
- Iron Mountain (USA)
- RWE (Germany)
- CLP Group (Hong Kong)
- Deutche Bahn (Germany)
- Intel (USA)
- NextDC (Australia)
- Solvay (USA)
- Procter & Gamble (USA)
- Mass Transit Railway (Hong Kong)



EPC Contractors:

- Worley (USA)
- Kapitol Group (Australia)
- Walbridge (USA)
- DPR (USA)

Consultants:

- PriceWaterhouseCoopers (Global)
- Deloitte (Global)
- KBR (Global)
- PTAG Inc (USA)
- RSGx (Australia)

2 Key Security, Privacy, and Compliance Features

2.1 Compliance and Certification

a. ISO 27001 Certified

b. ISO 27017 Certified

c. ISO 27701 Certified

d. Cyber Essentials Plus Certified

e. Fully UK and EU GDPR Compliant

2.2 Infrastructure Security

a. Leading cloud service providers (AWS, Azure)
b. Network: firewalls, intrusion detection systems, and network segmentation to prevent unauthorized access and protect against potential threats.
c. Web Application Firewall by Cloudflare (Gartner Magic Quadrant Leader)
d. Least-privilege, role-based access to production assets
e. In-transit encryption using TLS 1.2
f. At-rest encryption using AES-256 with AWS Key Management Service
g. Micro-service architecture in line with best practices
h. 99.5% SLA commitment

By implementing these cutting edge infrastructure security measures, we deliver a secure and reliable environment for our platform and the data it handles.

2.3 Security Features and Functionality

a. Integrates easily with Microsoft AD SSO
b. Role-Based Access Control (RBAC) – a robust and highly granular architecture to ensure appropriate level of access
c. Logging and Auditing: comprehensive logging and auditing mechanisms to monitor and track user activities and system events to enable effective incident investigation, compliance adherence, and proactive threat detection.

These security features and functionality contribute to a robust security posture by providing secure authentication, granular access controls, and detailed visibility into system activities.

2.4 Application Security

a. Secure Software Development Life Cycle (S-SDLC) to ensure that security is integrated into every phase of our software development process.
b. Risks managed against OWASP Top 10 methodology: We proactively identify and manage risks associated with the most critical web application security vulnerabilities outlined by OWASP.
c. Static code analysis: We REGULARLY scan and analyze our application's source code for potential security vulnerabilities and coding errors.
d. Regular penetration and configuration testing by third parties, including network scanning tools used against our production servers.

By integrating secure development practices, proactive vulnerability management, and regular third-party assessments, we strive to provide a secure and trustworthy software solution to our clients.

2.5 IT Security

a. Centrally managed EDR solution by SentinelOne for complete endpoint security.
b. Physical devices verified against UK Government-managed list of approved devices

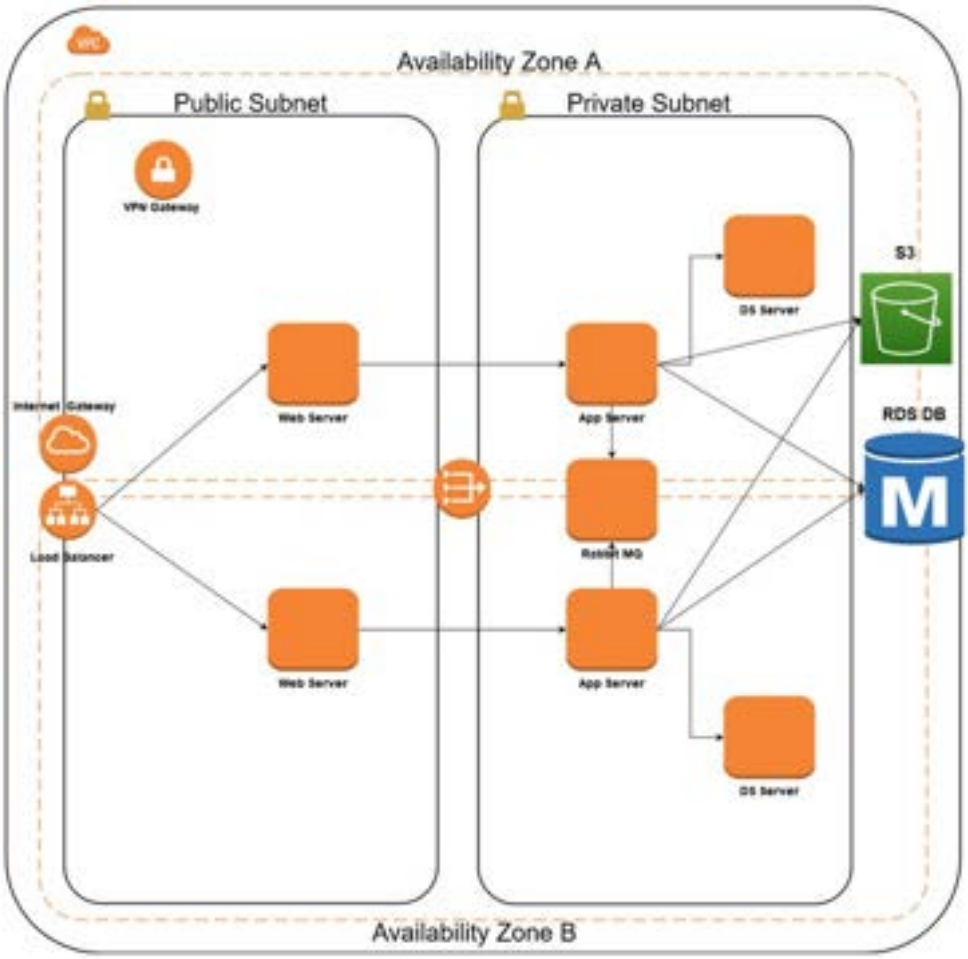
By implementing a robust endpoint security solution and validating physical devices against trusted sources, we enhance our overall security posture and protect against potential threats and vulnerabilities.

2.6 Operational Security

a. All employees cleated to UK Government's BPSS standard.
b. Key team security cleared to UK Governments' "Official Sensitive" level
c. Ongoing cybersecurity training and awareness

By promoting a culture of cybersecurity awareness, we empower our employees to be proactive in identifying and mitigating potential security risks, strengthening our overall security posture.

3 High-Level Cloud Architecture



CYBER SECURITY STRATEGY

1 Introduction

Foresight Works (FSW) is dedicated to building the central nervous system for the world's megaprojects. Our company serves megaproject owners by providing independent and unbiased data and insights to support their decision-making processes.

1.1 Company Services

FSW offers software-as-a-service solutions (SaaS Solutions) to provide megaproject owners with valuable data and insights. We are committed to delivering unbiased information that helps our clients make informed decisions throughout the project lifecycle.

1.2 Cloud Deployment Model

FSW utilizes a public cloud deployment model, leveraging virtualized resources for our SaaS Solutions. All maintenance and configuration activities are handled by FSW employees, primarily conducted remotely from our corporate office.

1.3 Logical Access Controls and Data Separation

To ensure the necessary separation of data from different clients, FSW implements logical access controls and maintains separate platforms. Our authentication and role-based access mechanisms ensure that data from each client is securely isolated. The infrastructure responsibilities lie with FSW's central system, known as Foresight. Additionally, clients have the functionality to manage their users and roles at the subscription level and make changes as needed.

1.4 Security Standards and Practices

FSW adheres to the ISO/IEC 27001:2013 standard and maintains compliance with Cyber Essentials Plus. Our operations follow industry-standard practices for operating highly secure SaaS solutions. This includes implementing security controls such as firewalls, intrusion detection systems, automated source-controlled configuration management, and formal security policies and procedures.

1.5 Employee Responsibilities for Information Security

At FSW, we recognize that information security is everyone's responsibility. Each employee is expected to comply with our information security policy to mitigate the ever-growing threats to information systems. We emphasize the protection of the company's information resources from destruction, alteration, or unauthorized access. By collectively upholding this policy, we ensure the appropriate safeguarding of our valuable assets.

By establishing these foundations and practices, FSW aims to provide secure and reliable services to our clients, protecting their data and ensuring the confidentiality, integrity, and availability of their information throughout the megaproject lifecycle.

2 Information Security Goals

2.1 Protecting Information

The primary objective of FSW's information security policy is to safeguard FSW employees, system users, and customers' information from unauthorized and malicious activity. By effectively and efficiently enforcing this policy, we ensure the confidentiality, integrity, and availability of sensitive information.

2.2 Enabling the Business Strategy

Our information security policy plays a crucial role in enabling the business strategy. It provides security and privacy guidance, along with risk management practices, to ensure the implementation of security measures aligns with the overall business objectives. By maintaining strong security and privacy practices, we can instill confidence in our customers and deliver exceptional customer service.

2.3 Maintaining Confidentiality, Integrity, and Availability

The information security policy is designed to uphold the confidentiality, integrity, and availability of information. We prioritize the protection of sensitive data from unauthorized access, alterations, or disruptions. By implementing robust security measures, such as access controls, encryption, and backup strategies, we maintain the trust of our stakeholders and ensure uninterrupted business operations.

2.4 Basis for Procedures and Controls

The information security policy serves as the foundation for establishing information security procedures and controls. It provides the framework and guidelines for implementing security controls, such as firewalls, intrusion detection systems, and data classification processes. By adhering to these procedures and controls, we mitigate risks and strengthen the overall security posture of our organization.

2.5 Managing Information Risks and Exposures

The policy guides the process of identifying, locating, and managing risks and exposures associated with information stored in the system. It encompasses not only digital information but also physical copies, including prints, scans, tapes, or other hard copies. By addressing the risks associated with information in all forms, we ensure comprehensive protection of sensitive data.

2.6 Annual Work Plan

The information security policy sets the required steppingstones for the development of an annual work plan. This plan outlines specific objectives, activities, and initiatives aimed at enhancing information security throughout the organization. By following this plan, we ensure a systematic approach to addressing security priorities, implementing necessary controls, and continuously improving our information security practices. Through the effective implementation of these policy objectives, FSW strengthens its information security posture, safeguards sensitive information, and aligns security practices with business strategies and customer needs.

3 Information Security Business Principles

3.1 Creating a Security Culture

FSW aims to foster a security culture throughout the organization through information security governance. This involves establishing clear roles, responsibilities, and accountability for information security. By promoting awareness, training, and communication, we ensure that all employees understand their roles in maintaining a secure environment and prioritize security in their daily activities.

3.2 Risk Assessment

Risk assessment is a fundamental component of our information security practices. We strive to understand, evaluate, and test potential risks to our systems, data, and operations. By conducting comprehensive risk assessments, we identify vulnerabilities and threats, prioritize risks, and implement appropriate controls and mitigation measures to reduce the likelihood and impact of potential security incidents.

3.3 Effective Implementation of Information Security Basics

To maintain a strong security posture, FSW emphasizes the effective implementation of critical information security basics. This includes following policies, procedures, and guidelines established by the organization. By adhering to these best practices, we ensure consistent and standardized security measures are in place across the organization.

3.4 Enforcing the Information Security Policy

Enforcement of the information security policy is crucial to maintaining a secure environment. FSW employs a multi-faceted approach to enforcement, including technological processes where applicable, education and training programs, ongoing monitoring, and metrics. By continuously monitoring and assessing security controls, we can promptly identify any deviations or potential security breaches and take appropriate actions to enforce the policy.

3.5 Adherence to Regulatory Requirements

FSW is committed to adhering to applicable regulatory requirements at both the international and state levels. This includes compliance with relevant laws and regulations governing information security, privacy, and data protection. By staying current with legal and regulatory changes, we ensure that our security practices align with the required standards and maintain compliance with legal obligations.

By focusing on these objectives, FSW establishes a strong information security governance framework, assesses and mitigates risks, implements effective security measures, enforces policies, and complies with applicable laws and regulations. This holistic approach fosters a security culture, protects valuable assets, and instils confidence in our stakeholders.

4 Product Security and Data protection:

4.1 Security Architecture Validation

At FSW, security is a core principle in the design and review of our architecture. Our team consists of experienced security experts who have designed the product and its architecture from the ground up, ensuring that security considerations are integrated throughout the development process. This approach validates the security architecture and ensures the implementation of robust security measures.

4.2 Infrastructure on AWS Cloud

FSW's infrastructure is built on the AWS cloud platform, eliminating the need for physical servers or network equipment at our physical offices. By leveraging the secure and scalable infrastructure provided by AWS, we can ensure high availability, reliability, and strong security controls for our platform.

4.3 HTTPS Traffic for Customer Access

To ensure the secure transmission of data, all traffic related to requests to access customers' resources is done over HTTPS. Hypertext Transfer Protocol Secure (HTTPS) encrypts the communication between users and the FSW platform, protecting sensitive information from unauthorized interception or tampering. This security measure ensures the confidentiality and integrity of data transmitted between users and our platform.

4.4 Authentication and Access Management

4.4.1 The access to the FSW platform is done through 2-factor authentication. A strong password of at least eight characters and a verification link are sent to the user's email to accommodate the user's first login.

4.4.2 Within the FSW backend, all resource access is based on IAM roles with minimum permissions.

4.5 Data collected/retained.

4.5.1 FSW's platform collects:

- HTTP requests/responses to 3rd-party service.
- Managed BI data pf projects

4.5.2 The Foresight. Works backend collects additional logs and metrics and uses them to enrich the analytics presented on the FSW platform.

4.5.3 All data is relayed back to FSW backend in a secure manner over HTTPS.

4.6 Encryption/protection

4.6.1 All of the FSWs' data is retained at AWS data centers in a secure environment according to best practices.

4.6.2 All data transmitted between FSW and its users is protected using Transport Layer Security (TLS)

4.7 Data retention

4.7.1 Users can ask for their data to be deleted at any time.

4.7.2 We do not sell or license information, recordings or any other form of data to anyone.

5 Key elements in establishing an ISMS

Information security measures and methods are generally implemented to minimize risks and based on the risk and sensitivity level over time.

5.1 Prevention – information security components are designed to prevent malicious or accidental damage to a company's information by employees or outsourcers, such as access control systems, authorization systems, and anti-virus software.

5.2 Detection – detecting breaches that were not identified by the prevention layer.

5.3 Reaction – a reaction (or correction) layer that may be independent or part of the detection layer. Allows response to the breach as a function of the event:

Real-time reaction – by changing the prevention capabilities of the system.

Post-event reaction – Based on information logged during the event, analyzing of it, and drawing conclusions.

5.4 Documentation – the documentation layer allows analyzing of the events (prevention, detection, or reaction events) to allow a broad perspective.

6 Risk Assessment approach

A periodic risk assessment is a basis for an ongoing information security activity and roadmap. The assessment applies to the technological and non-technological aspects of information security.

The risk assessment includes internal and external tests, penetration tests, system configuration reviews etc., and represents risks based on the potential risk and occurrence likelihood. The assessments and surveys are performed according to business requirements and professional advice.

7 Security of Human Resources

FSW implements various aspects of information security throughout the procedures and stages of employing employees. The following measures are implemented to ensure the security of human resources:

7.1 Before Employment of Employees:

7.1.1 Suitability and Understanding of Responsibilities: FSW ensures that prospective employees, as well as third-party employees (contractors), are suitable for the intended positions and have a clear understanding of the responsibilities imposed on them.

7.1.2 Employee Reliability: FSW determines employee reliability through a thorough process that includes multiple interviews and gathering of recommendations to assess the candidate's background and qualifications.

7.1.3 Confidentiality Agreement: Each employee is required to sign a confidentiality agreement, acknowledging their commitment to maintain information security and privacy rules as a condition of their employment with FSW.

7.1.4 Security and Privacy Training: Before commencing work, new employees undergo security and privacy training to familiarize themselves with FSW, its policies, and the quality and information security documents. This ensures that employees are aware of their roles and responsibilities in maintaining information security.

7.2 During the Employment Process:

7.2.1 Employee Awareness: FSW management is responsible for ensuring that all employees, including third-party employees, are aware of information security threats, their responsibilities, and the information security policy and related procedures. This helps prevent unintentional or malicious failures in information security.

7.2.2 Periodic Training: The information security manager conducts periodic training sessions, at least once a year, to increase employee awareness of the information security policy and associated risks. These training sessions keep employees up to date with best practices and emerging threats.

7.3 Completion of Employment or Change of Positions:

7.3.1 Orderly Departure or Change of Positions: FSW management is responsible for ensuring that employees, contractual employees, or third-party users of the information systems leave the organization or transition to new positions in an orderly and secure manner. This includes proper handover of responsibilities and revoking access rights as necessary.

7.3.2 Access Authorization Review: When an employee transitions to a new position, FSW examines their access authorizations and controls, taking into consideration the new authorizations required for their new role. This helps ensure that access privileges are aligned with the employee's responsibilities and that any unnecessary access rights are revoked.

By implementing these measures throughout the employment lifecycle, FSW aims to ensure that employees are suitable for their positions, are aware of their information security responsibilities, and adhere to the information security policies and procedures. These practices contribute to a secure working environment and protect the organization's sensitive information.

8 System Access Control

FSW implements robust access control measures to safeguard its information systems. The following practices are in place to ensure secure access to the company's systems:

8.1 End-User Passwords:

8.1.1 Strong Passwords: Passwords for all the company's information systems are required to be at least eight characters long and include a combination of alphanumeric characters. This ensures that passwords are not easily guessable, enhancing the security of user accounts.

8.1.2 Strong Authentication: Access to the internal network and sensitive services is based on strong authentication methods. This may include multi-factor authentication (MFA) or other mechanisms that provide an additional layer of security beyond passwords alone.

8.1.3 Secure Password Storage: FSW provides a secure password storage solution to all employees. This helps protect passwords from unauthorized access and ensures that they are stored securely using industry-recognized encryption and hashing techniques.

8.2 Accounts Management:

8.2.1 Password Access Controls: All information systems connected to FSW's networks, whether permanently or intermittently, have password access controls. This ensures that user accounts are protected by passwords and helps prevent unauthorized access.

8.2.2 Principle of Least Privilege: When creating and maintaining user accounts, the principle of least privilege is followed. Users are granted only the permissions necessary to perform their specific job functions, reducing the risk of unauthorized access or misuse of system privileges.

8.2.3 Re-Authorization of Non-Company Employees: Access for non-company employees, such as contractors or third parties, is re-authorized annually. This ensures that access rights are reviewed and updated regularly, taking into account changes in employment status or project requirements.

8.2.4 Regular Privilege Evaluation: System privileges granted to every user are re-evaluated by managers every 180 days. This periodic evaluation ensures that user access rights are still aligned with their job responsibilities and the principle of least privilege.

8.2.5 When authorized users are terminated or leave the company, their access is immediately terminated.

By implementing these system access control measures, FSW ensures that strong passwords protect user accounts, access is based on strong authentication, and user privileges are granted and reviewed based on the principle of least privilege. These practices contribute to a secure access control environment and help prevent unauthorized access to FSW's information systems.

10 Software Security

FSW prioritizes software security to ensure the integrity, legality, and security of software used within the organization. The following practices are implemented:

10.1 License Management

FSW strongly emphasizes strict adherence to software vendors' license agreements and copyright holder's notices. This includes ensuring that all software used within the organization is properly licensed and compliant with the terms and conditions set by the software vendors. FSW takes measures to track and manage software licenses to maintain legal and ethical practices.

10.2 Third-Party Software Product Security

Before the installation of any software required by company employees, a review and authorization process is conducted by the Information Security Manager. This ensures that all software installations undergo a thorough assessment, considering security aspects, such as vulnerability assessments, code review, and adherence to secure coding practices. By reviewing and authorizing software installations, FSW minimizes the risk of introducing potentially insecure or vulnerable software into the organization's environment.

10.3 SaaS Solutions Security

10.3.1 Approval and Vendor Assessment

For the usage of third-party services, the approval of the Information Security Manager is required. Each service is assessed for its security measures and vendor statements to ensure they align with industry standards and best practices. This assessment includes evaluating the service's security controls, data protection measures, compliance certifications, and incident response capabilities.

10.3.2 Securing Sensitive Data Services

All tsensitive data services used by FSW employees for business processes undergo vetting by the Information Security Manager. These services are configured to support the highest level of security supported by the product, with a focus on managing permissions and securing authentication. By carefully configuring and securing these services, FSW ensures the protection of sensitive data and reduces the risk of unauthorized access or data breaches.

By implementing these software security measures, including license management, review and authorization of third-party software installations, and securing SaaS solutions, FSW enhances the overall security of its software environment. These practices contribute to the protection of company assets, the prevention of software license violations, and the promotion of secure software usage within the organization.

11 Physical Security

11.1 Access Security to FSW Offices

FSW ensures that access to the company's offices is secured and monitored at all times. This includes implementing appropriate measures to control entry and monitor access activities, contributing to a safe and secure environment.

11.2 Security in Work Areas

11.2.1 Remote Work Considerations: FSW employees work from various locations, including home or public places. It is emphasized that employees should always keep their laptops with them, ensuring the security and protection of company assets and data.

11.2.2 Laptop Security: FSW employees are required to lock their laptops using a password-protected screensaver whenever they leave their workstation unattended. This practice helps prevent unauthorized access and protects sensitive information from being exposed.

11.2.3 Vacation Protocols: When employees go on vacation, they are instructed to either turn off their computers or put them into hibernation mode. This helps ensure that encryption sequences are activated, providing an additional layer of protection for sensitive data.

11.2.4 Paperless Culture: FSW promotes a paperless culture, except when it involves marketing and sales materials intended for public or potential customer and partner disclosure. This approach reduces the risk of physical document mishandling and enhances data security.

11.3 Proper Disposal of Physical Information

FSW maintains proper procedures for the disposal of physical information that contains non-public information. Paper documents with confidential content are shredded or placed in a secured shred

11.3 Proper Disposal of Physical Information

FSW maintains proper procedures for the disposal of physical information that contains non-public information. Paper documents with confidential content are shredded or placed in a secured shred bin to prevent unauthorized access or data leakage. Removable media that contains sensitive information is controlled until the data has been erased or the physical media has been securely destroyed. These disposal practices ensure the appropriate protection and confidentiality of sensitive information.

By implementing these security measures related to work areas and the proper disposal of physical information, FSW aims to protect sensitive data, maintain confidentiality, and minimize the risk of unauthorized access or data breaches. These practices contribute to maintaining a secure work environment and safeguarding company assets and information.

12 Reporting of Security Incidents

FSW recognizes the importance of timely reporting and taking corrective actions in response to information security incidents. The following practices are in place to ensure effective incident management:

12.1 Forensics and Reporting of Communications Crimes

If evidence clearly indicates that a computer has been a victim of a communications crime, the Information Security Manager promptly conducts appropriate forensic investigations. This includes gathering evidence, analyzing the incident, and identifying the scope and impact of the security breach. The Information Security Manager also assists with reporting the incident to relevant authorities or law enforcement agencies as necessary, in accordance with applicable laws and regulations.

12.2 Retention of Information Security Incident Reports

FSW retains information related to all reported information security problems and violations for a period of two (2) years. This includes incident reports, documentation, and any supporting evidence. By retaining this information, FSW ensures a comprehensive record of incidents, enabling effective analysis, trending, and identification of patterns or recurring issues. This information also assists in auditing, regulatory compliance, and continuous improvement of security practices.

These practices demonstrate FSW's commitment to promptly addressing and managing information security incidents. By conducting forensic investigations, reporting crimes when necessary, and retaining incident-related information, FSW enhances its ability to respond to incidents, learn from them, and implement corrective actions to prevent future occurrences.

13 Malware

13.1Malware

13.1.1 Workstation Virus-Screening Software

To ensure the uninterrupted service of all information systems, all workstations at FSW are equipped with approved virus-screening software. This software helps detect and prevent the spread of viruses, malware, and other malicious software. It is mandatory for all removable media to be scanned for viruses before being used on any information system. Disabling the antivirus software is strictly prohibited and may result in disciplinary actions, including termination.

13.1.2 Server Protection

FSW's server protection strategy includes several measures. Outbound access is carefully managed to allow only permitted connections, minimizing the risk of unauthorized access or data exfiltration. Automatic security patching is implemented to ensure that servers are up to date with the latest security patches and fixes, reducing vulnerabilities. Additionally, automated monitoring systems are in place to detect Command & Control instances, which could indicate a security compromise. This proactive approach helps identify and respond to potential security threats promptly.

13.1.3 Endpoint Virus Definition Updates

To stay protected against the latest threats, endpoints at FSW have an automatic update mechanism for virus definition files. These files, issued by the antivirus software vendor, contain information about the latest known threats and their signatures. By automatically updating these definition files as soon as they are released, FSW ensures that endpoints have the most up-to-date protection against known viruses and malware.

By implementing these measures, including workstation virus-screening software, server protection measures, and automatic virus definition updates, FSW strengthens its overall security posture. These practices help minimize the risk of malware infections, protect against emerging threats, and ensure that systems and data remain secure and resilient