FORTERRO

INFORMATION SECURITY DOCUMENT

November 2023

Document Ref.	Information Security Document
Version:	0.9
Dated:	01 November 2023
Document Author:	David Adams
Document Owner:	Richard Dunn

Revision History

Version	Date	Revision Author	Summary of Changes
0.1	11/04/2022	David Adams	Original/Draft
0.2	20/05/2022	David Adams	Initial Review
0.3	15/09/2022	Polly Eldridge	Legal Review
0.4	30/09/2022	Rob Hallmark	Legal Review
0.5	03/10/2022	Polly Eldridge	Legal Review
0.6	06/10/2022	Rob Hallmark	Legal Review & Comments from David Adams (via call)
0.7	15/05/2023	David Adams	Updated planned dates
0.8	29/09/2023	David Adams	Updated planned dates
0.9	01/11/2023	David Adams	Updated to new branding

FORTERRO

Table of Contents

Forterro Information Security Framework

How information is handled by the Forterro Group and third parties on our behalf is of the upmost importance to our business and its people.

Document Objective

This Information Security Framework Document (**Security Framework**) provides an overview of the measures implemented at the Forterro Group (**Forterro**) concerning information security in the provision of our products and services. This Security Framework also details how we approach our information security measures with third parties who may process information on our behalf.

DISCLAIMER: this Security Framework is intended for informational purposes only. Nothing in this Security Framework is a contractual or binding commitment and Forterro hereby disclaims any liability whatsoever in connection with this Framework and its use (or otherwise). Forterro reserves the right to modify this Security Framework and the underlying processes at Forterro at any time.

A copy of this document (as may be updated) will be made available on request.

You can also find the privacy policy of Forterro at the following link:

https://www.forterro.com/en/company/privacy-policy

Our Security Framework Objectives

At Forterro we invest in the protection of our customer information. We have detailed security processes and secure systems, specific user access control with other measures such as virus control, password access and authentication, incident handling, secure communications and encryption all designed to prevent a breach of information security. We consider a breach to an incident that causes or even risks the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or unauthorised access to any customer data whether transmitted, stored by us or otherwise processed by us or on our behalf. We approach our investment in a number of ways, such as:

- information security training to all our employees and others who require it;
- report and investigate information incidents in accordance with our incident reporting procedure;
- monitor compliance with our information security policies;
- create, maintain and test our business continuity plans and update our systems to endeavour to protect against malicious activity and attacks; and

- adopt industry-leading techniques to ensure that all relevant employees follow the Forterro procedures and adhere to our standards.

Our approach to information security is a continuous drive to adapt the technical and organisational measures in place across Forterro with the goal of ensuring a level of security exists that is appropriate to the risks in practice.

Our Security Committee

Data protection and information security is overseen at the highest employee level at Forterro led by our *Forterro Information Security and Governance Committee* (**the Security Committee**). The Security Committee approve and maintain the Forterro internal policies (**the Security Policies**) which cover all information security and data protection requirements relating to the Forterro business, products and services.

This Security Committee meets at least quarterly and includes:

- Chief Executive Officer (CEO)
- Chief Technical Officer (CTO)
- Chief Financial Officer (CFO)
- Chief Legal Officer (CLO)
- Chief Services Officer (CSO)
- The SVP IT & Cloud Ops
- VP IT Security

There are 3 specific internal policies that are of central importance to our detailed Information Security Management System (**the Forterro ISMS**). These 3 policies are:

- Forterro Group Data Classification & Handling Policy – this defines the roles and responsibilities for compliance and data protection for Forterro, this policy also details the requirements for carrying out data protection and risk assessments for all proposed projects that will have an impact on the handling or use of personal data.
- Acceptable Use and Information Security Policy Summary – this policy defines the standards all personnel involved with Forterro must follow for acceptable conduct concerning security controls.
- Forterro Incident Response Procedure – defines the reporting and investigation procedure for all security incidents that become known or are reported to anyone within Forterro.

All Security Policies are supplied to all internal and relevant external individuals working for or on behalf of Forterro and are delivered by an online training and policy management platform via the ISMS. Product owners at Forterro who are responsible for delivering the Forterro products and services are also primarily responsible for implementing these policies at that local level as well as

monitoring local compliance with these policies. Security Policies are updated by Forterro when necessary, and usually no less than on an annual basis.

Forterro Controls

Forterro ISMS

The Forterro ISMS is used at Forterro as on online platform for collating, developing and sharing internal documentation and other communications concerning the Security Policies. The Forterro ISMS also delivers a dedicated online personnel training centre with bespoke measurement tools to support the evaluation of such training and the effective level of understanding demonstrated across all the relevant Forterro personnel. All Forterro products and services must adhere to and comply with the applicable standards of the Forterro group as laid out in the Forterro ISMS.

Organisational Security

A dedicated Forterro product manager (**the Product Manager**) will be allocated to each Forterro customer and will act as the point of contact for all routine customer information security and data protection enquiries. The Product Manager will engage with all personnel delivering the Forterro products and services to our customers and oversees the compliance with our Security Polices.

The Forterro organisation also operates with certain key management roles that together form a robust support team to supervise the ongoing operation and implementation of the Security Policies across Forterro (**the Security Team**). The Security Team works alongside the Product Managers and the Security Committee and comprises of the following:

- R&D Manager
- Support Manager
- VP IT Operations
- VP IT Security

Risk Assessments

Forterro, in conjunction with its Security Team and others, endeavours in the undertaking of relevant, appropriate and timely risk assessments to identify and avert potential information breaches (and other incidents) from occurring anywhere across the Forterro Group, its products and its services. The Forterro systems are regularly reviewed against the Security Policies with further controls and control objectives and any discrepancies identified and plans for remediation drawn up.

Asset Register

The Forterro IT Operations Director also records and maintains a register of all assets (including acquired software licences) in a dedicated assets register system (**the Asset Inventory**) in order to enhance the transparency and robustness of the Forterro information security system.

Data Classifications

Where relevant to the Forterro products and services, the presence of any personal data being processed, stored or transmitted by us or on our behalf is handled in accordance with the relevant categorisation of such personal data and the treatment of such personal data is also subject to Forterro legal team oversight.

Technical Compliance Review

The Forterro systems operating with our products and services are assessed during creation and also during any updates for vulnerabilities that can be identified. A further 'Pen' test is carried out every year and for releases of any major updates or new versions as part of any software development life cycle.

Personnel

Employees and any other relevant personnel working for or on behalf of Forterro may have access (depending on the nature of their role) to personal data stored in the 'Cloud' or otherwise. The following steps describe the main requirements at Forterro concerning these personnel who have, or might have, access to any personal data of any kind.

Prior to employment

- Forterro personnel involved in the delivery of services to our customer are subject to background checks and verifiable references to assess suitability in accordance with existing policies.
- All personnel are required to understand and accept each of the Security Policies (as are described in more detail further above).

During employment

- Each of the Security Policies (and any associated requirements) apply to all personnel with the ability to access any personal data.
- The Security Policies are communicated to all personnel through a mandatory training program provided by the Forterro ISMS, and such users are tested to confirm the level of their understanding and required to sign that they will comply with these policies.
- Production procedural training is carried out by Forterro itself and must be undertaken before an employee is allowed to operate in the production environment.

Termination of employment

- When an employee gives notice to leave Forterro or is otherwise given notice by Forterro to terminate their employment contract, a ticket is raised in the Forterro's Service Desk by HR, which notifies the relevant IT department of the employee's impending departure and to commence the appropriate next steps.
- At the leaving date of an employee, the relevant Forterro IT department terminates the individual's access to all of Forterro's networks and systems and completes the returns process for all IT equipment registered in the Asset Inventory in communication with the Employee's relevant HR and IT representatives to ensure safe collection of all the employee's IT equipment (and any other assets) belonging to Forterro and return to the central corporate IT function for further processing.
- Following departure of an employee from Forterro, the relevant Forterro employment contract for each individual is designed to retain appropriate obligations on such employee to continue to maintain confidentiality for the relevant period concerning information pertaining to Forterro, including its services, customers, systems and products.

Change of employment

- Upon any change of role for an employee within Forterro, the relevant HR team raises a ticket in the Forterro Service Desk system which is then used by the Forterro IT department to determine if any user permissions need to be adjusted or revoked or additional rights granted in any of Forterro's networks and systems accordingly.

Provisional dates for the completion of tasks ahead

Tasks	Provisional Date
Addition of Managed Detect and response Service to supplement the AWS Security which includes forensic capture etc	End of Q2 2024
Revised Policies and Procedures Review and Additions to make compliance with the Centre for Internet Security framework V8 and ENISA	End of Q3 2023 Complete
Procedures supporting the revised Policies	End of Q2 2024
Information Vulnerability Disclosure program	End of Q1 2024

The individual user software control is being consolidated to use a single tool and roll out will start before the end of the year, Data centre controls are already in place	End of Q3 2023 Complete
Upgrading of Static Code Analysis solution	End of Q3 2023 Complete

FORTERRO

Cloud Security Specific Information

Type	Description	Security Measures
ERP SaaS	Cloud based that is easy to implement and use, while still delivering the functional depth and expert services required by industrial companies. When manufacturers choose Forterro, they are choosing modern, open, and configurable ERP software solutions that are ideal for supporting them in the evolution of their business model, as well as the digitization of their plant.	Containerized architecture, which provides customers with leading scalability, availability and also security.

- PASSWORD STRENGTH POLICY
  Password policy is enforced by the software, as follows:
  Hosted: Configurable, length, number, uppercase, special characters.
  Cloud Fixed: Minimum length of 14, uppercase letters, lowercase letters, special characters, numbers.

- MULTI-FACTOR AUTHENTICATION
  Multifactor Authentication is available on cloud version. The administrator can enforce MFA for all users.

- HOW ARE PRIVILEGED USERS ASSIGNED
  All access, included administrator rights, are granted via roles assigned to a user account, with the exception of a Support Service account for use by support.

- ROLES
  The different roles and the permissions are described in the application.

- ADMINISTRATION
  The Customer administrator can manage users, roles and access for the customer's employees within the application.

- CONFIGURATION CHANGES
  The customer is able to make changes themselves within the product, and is online documentation provides instruction to setup access etc.

- AUTHENTICATION OF USER ACCESS CHANGE REQUESTS
  The Customer administrator can make all of these changes without requiring Forterro to do this for them. For support to engage with a customer the request must be initiated customer email form an authorised contact.

- USER REGISTRATION AND DE-REGISTRATION
  Users' registration and de-registration activities can be managed by the customer administrator.

- MANAGEMENT OF PRIVILEGED ACCESS RIGHTS
  Apart from the initial administration user creation for a new customer, the customer is able to administer all of the users within the system, the privileges are assigned through a role being assigned to an account in the system.

- MANAGEMENT OF PASSWORD AUTHENTICATION INFORMATION OF USERS
  For an on-premise environment (that we host on behalf of the customer in the Cloud) a Customer Administrator has the ability to update a staff members password.
  For a Cloud service the user's password cannot be modified by the administrator as there is a user password reset function.

- REVIEW OF USER ACCESS RIGHTS
  The review of customers users access rights is the responsibility of the customer.

- REMOVAL OR ADJUSTMENT OF ACCESS RIGHTS
  The responsibility for the removal of Customer staff or the adjustment of a customer employee's permissions following a change of job is the responsibility of the customer.

- ENVIRONMENT SECURE LOG ON PROCEDURES
  Forterro implements a 'Just in Time Permission' approach through the Microsoft Privileged Access Management tooling with accounts separate from a user's normal day to day login.

- ENVIRONMENT PASSWORD MANAGEMENT SYSTEM
  Forterro enforces its password policies through its Privileged Identity Management system to enforce complex passwords. Service account passwords are kept in a key vault that is queried at run time by services that need to operate.

- ACCESS TO PROGRAM SOURCE CODE
  Strictly controlled and undergoes a rigorous process of review before code can be checked back into the main code line. A robust Software Development Life cycle is implemented to make use of Static code analysis for vulnerabilities, Training of staff in how to code securely, peer reviews and Pen testing mechanisms are employed.

For the avoidance of doubt, Forterro Cloud products will not seek to circumvent, compromise or change the Client's security controls, and Forterro Cloud products will not change the Client's software configurations (without proper authorisation).

Encryption (Cryptography)

Data is encrypted at rest and when in transit using the Amazon Web Services (**AWS)** storage mechanisms and Https with TLS cryptography.

Forterro Cloud physical and environmental security

The Forterro service is hosted in AWS Data Centres and as such the physical security is covered by the AWS Infrastructure security in accordance with ISO 27001 and HDS (Health Data Hosting) in alignment with the shared responsibility model - https://aws.amazon.com/compliance/shared-responsibility-model

Full and up to date details of the AWS Controls can be found on this link: Data Centres - Our Controls (amazon.com)

- EMPLOYEE DATA CENTER ACCESS
  AWS provides physical data centre access only to approved employees. All employees who need data centre access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data centre the individual needs access and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions.

- THIRD-PARTY DATA CENTER ACCESS
  Third-party access is requested by approved AWS employees, who must apply for third-party access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data centre the individual needs access and are time-bound. These requests are approved by authorized personnel, and access is revoked after request time expires. Once granted admittance, individuals are restricted to areas specified in their permissions. Anyone granted visitor badge access must present identification when arriving on site and are signed in and escorted by authorized staff.

- AWS GOVCLOUD DATA CENTER ACCESS
  Physical access to data centres in AWS is restricted to AWS employees.

- REDUNDANCY
  Data centres are designed to anticipate and tolerate failure while maintaining service levels. In case of failure, automated processes move traffic away from the affected area. Core applications are deployed to an N+1 standard, so that in the event of a data centre failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

- AVAILABILITY
  AWS has identified critical system components required to maintain the availability of our system and recover service in the event of outage. Critical system components are backed up across multiple, isolated locations known as Availability Zones. Each Availability Zone is engineered to operate independently with high reliability. Availability Zones are connected to enable you to easily architect applications that automatically fail-over between Availability Zones without interruption. Highly resilient systems, and therefore service availability, is a function of the system design. Through the use of Availability Zones and data replication, AWS customers can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability.

- CAPACITY PLANNING
  AWS continuously monitors service usage to deploy infrastructure to support our availability commitments and requirements. AWS maintains a capacity planning model that assesses our infrastructure usage and demands at least monthly. This model supports planning of future demands and includes considerations such as information processing, telecommunications, and audit log storage.

- BUSINESS CONTINUITY PLAN
  The AWS Business Continuity Plan outlines measures to avoid and lessen environmental disruptions. It includes operational details about steps to take before, during, and after an event. The Business Continuity Plan is supported by testing that includes simulations of different scenarios. During and after testing, AWS documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement.

- PANDEMIC RESPONSE
  AWS incorporates pandemic response policies and procedures into its disaster recovery planning to prepare to respond rapidly to infectious disease outbreak threats. Mitigation strategies include alternative staffing models to transfer critical processes to out-of-region resources, and activation of a crisis management plan to support critical business operations. Pandemic plans reference international health agencies and regulations, including points of contact for international agencies.

Equipment

- EQUIPMENT SITING AND PROTECTION
  Prior to choosing a location, AWS performs initial environmental and geographic assessments. Data centre locations are carefully selected to mitigate environmental risks, such as flooding, extreme weather, and seismic activity. Our Availability Zones are built to be independent and physically separated from one another.

- PROTECTION AGAINST POWER FAILURES AND DISRUPTIONS
  AWS data centre electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. AWS ensures data centres are equipped with back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility.

- CLIMATE AND TEMPERATURE
  AWS data centres use mechanisms to control climate and maintain an appropriate operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages. Personnel and systems monitor and control temperature and humidity at appropriate levels.

- FIRE DETECTION AND SUPPRESSION
  AWS data centres are equipped with automatic fire detection and suppression equipment. Fire detection systems utilize smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas are also protected by suppression systems.

- LEAKAGE DETECTION
  In order to detect the presence of water leaks, AWS equips data centres with functionality to detect the presence of water. If water is detected, mechanisms are in place to remove water in order to prevent any additional water damage.

- PROTECTION OF CABLING FROM INTERCEPTION, INTERFERENCE OR DAMAGE
  AWS data centres are connected to major internet backbones and are monitored for any disruptions of service.

Equipment Maintenance

- AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centres. Equipment maintenance procedures are carried out by qualified persons and completed according to a documented maintenance schedule.

Removal of Assets

- ASSET MANAGEMENT
  AWS assets are centrally managed through an inventory management system that stores and tracks owner, location, status, maintenance, and descriptive information for AWS-owned assets. Following procurement, assets are scanned and tracked, and assets undergoing maintenance are checked and monitored for ownership, status, and resolution.

- SECURE DISPOSAL OR RE-USE OF EQUIPMENT, MEDIA DESTRUCTION
  Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned.

Media Handling

- REMOVABLE MEDIA
  Removable media is not permitted in the datacentre.

- MEDIA DESTRUCTION
  Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned.

Documented Operating Procedures

- PROCEDURES
  A Procedure repository is used to store the procedures for administering the cloud infrastructure, building, troubleshooting/extending storage clusters, data migration, software updates, backups etc.

- CHANGE MANAGEMENT
  A Change Management Process is in place with tickets being created for every change in our service desk tool with a Change Advisory Board convened to assess the impact and approve changes.

- CAPACITY MANAGEMENT
  The use of resources is monitored, tuned, evaluated and future capacity and usage requirements are calculated to ensure systems continue to perform at optimum levels.

- SEPARATION OF DEVELOPMENT, TESTING AND OPERATIONAL ENVIRONMENTS
  Air gaped separate environments are used for Development/Testing and Production and access to production is not permitted for Dev/QA teams.

- PROTECTION FROM MALWARE
  The production environment is a private cloud instance using containerized instances, that are protected using an Antivirus tool and undergo vulnerability scanning on a regular basis, the network is private and protected behind firewalls. Telemetry is fed to a Security Information and Event Management tool and Network Intrusion/protection systems are implemented and Monitored by a 24/7/365 Security Operations Centre.

Back-Up

- BACKUP
  External air gapped full backups are created every week with incremental backups on the intervening days. Hourly snapshots are carried out in order to further improve recovery point.

- EVENT LOGGING
  All logs are sent to the SIEM tool for correlation and as a matter of record.

- PROTECTION OF LOG INFORMATION
  Logs once sent to the SIEM cannot be changed or updated.

- ADMINISTRATOR AND OPERATOR LOGS
  Logs of all activities are captured in the SIEM tool and act as a matter of record, an administrator account also requires a Just in Time authorization in order for their account to be activated, and this is also audited.

- CLOCK SYNCHRONISATION
  All of the environments are configured with an NTP service so the clocks are accurate.

- CONTROL OF OPERATIONAL SOFTWARE
  The environment is configured to use containers which are built through configuration code which defines what software is installed and how it is configured.

- MANAGEMENT OF TECHNICAL VULNERABILITIES
  Forterro uses vulnerability feeds from security partners to identify products with newly discovered vulnerabilities and uses this to address any necessary updates and patches in line

with its release and Change management processes. Pen tests are also used to ensure the product is tested for vulnerabilities prior to release.

- RESTRICTIONS ON SOFTWARE INSTALLATIONS
  The installation of software is controlled in code within the Datacentres and for end users a separate tool is employed to control approved versions of software.

Communications security

- NETWORK CONTROLS
  AWS operates stringent controls to stop and detect attempted unauthorised access of the environments.
  Forterro have also added a Security Information and Event Management tool which is a manned 24*7*365 Security Operations Centre that is constantly monitoring for any unauthorised access.

- SECURITY OF NETWORK SERVICES
  AWS security monitoring is maintained and reviewed on a regular basis, Forterro monitors network security with regular reviews to ensure the effectiveness of the service.

- SEGREGATION OF NETWORKS
  Production networks are air gapped from corporate and dev/test environments.

- ELECTRONIC MESSAGING
  Forterro Acceptable Use and Information Security Policy Summary has statements that cover the acceptable use of email and instant messaging technologies.

- CONFIDENTIALITY OR NON-DISCLOSURE AGREEMENTS
  When contracting with a third-party Forterro ensures that the Legislative requirements for handling data are covered contractually.

- HOW WE TRANSMIT CONFIDENTIAL INFORMATION TO CUSTOMERS
  Confidential information is shared with customers through a separate SharePoint instance where permissions are created using the customers identity provider.

- INFORMATION TRANSFER POLICIES AND PROCEDURES
  Forterro has the Forterro Group Data Classification & Handling Policy that covers how data should be handled in line with the relevant legislative requirements.

System acquisition, development and maintenance

- INFORMATION SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION
  Forterro conducts a rigorous review of any new systems that it looks to introduce to ensure they are secure and meet the legislative requirements.

- PROTECTING APPLICATION SERVICES TRANSACTIONS
  Data is transferred to and from the Forterro application over HTTPS making use of TLS encryption.

Security in development and support processes

- SECURE DEVELOPMENT POLICY
  All new application development follows a common set of security guidelines.

- SYSTEM CHANGE CONTROL PROCEDURES
  All development on products includes control procedures through usage of GIT version control system.

- TECHNICAL REVIEW OF APPLICATIONS AFTER OPERATING PLATFORM CHANGES
  The testing environment and processes include retesting after operating system updates.

- RESTRICTIONS ON CHANGES TO SOFTWARE PACKAGES
  Changes to Forterro code or third-party packages are controlled and go through the Software Development life cycle for testing and the Change Management Process.

- SECURE SYSTEM ENGINEERING PRINCIPLES
  Common system security principles are applied and documented.

- SECURE DEVELOPMENT ENVIRONMENT
  The development and test environments have security controls in place to control access and limit it to authorised personnel, version control is also applied to these dev and test environments.

- OUTSOURCED DEVELOPMENT
  Where code has been outsourced, the process ensures licencing and ownership is retained by Forterro, and the code is tested and investigated for any security issues.

- SYSTEM SECURITY TESTING
  Application security testing is part of the Software Development Life Cycle that Forterro uses. A Security audit is also carried out for every major release by an external independent company.

- SYSTEM ACCEPTANCE TESTING
  Acceptance testing is part of the software development lifecycle that Forterro uses with a combination of automatic and manual testing.

Test data

- PROTECTION OF TEST DATA
  The data that is used for testing is anonymized and is compliant with the GDPR requirements.

Supplier relationships

- INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS
  Any third parties that are contracted to work as a Forterro Partner are required to sign up to the Forterro policies and standards.

- ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS
  The third-party suppliers/Partners to Forterro have security clauses tied into the commercial agreements duly put in place between each of them and Forterro.

- INFORMATION AND COMMUNICATION TECHNOLOGY SUPPLY CHAIN
  Forterro, as part of its contracts and controls, takes reasonable steps to ensure that third parties that are involved in the support of the service to contribute Libraries to the Forterro Product have processes and procedures to address the information security risks associated with the information and communications technology services and product supply chain.

Supplier service delivery management

- MONITORING AND REVIEW OF SUPPLIER SERVICES
  Forterro looks for Partners with accreditations that are regularly reviewed to ensure that the services that are used are reliable and have monitoring in place to measure any deviations from the service availability.

- MANAGING CHANGES TO SUPPLIER SERVICES
  Forterro has a set of Policies that govern the use of third parties and the services that are procured through them, any changes would need to go through the Change Management Process to be appropriately reviewed and assessed.

Information security incident management

- RESPONSIBILITIES AND PROCEDURES
  Forterro has an incident response plan which covers the Forterro product set, the plan defines the procedures for responding to an incident along with the roles and responsibilities during and after the incident.

- REPORTING INFORMATION SECURITY EVENTS
  The Forterro incident response plan defines the communications plan for informing management of incidents and the time frames that that communication needs to happen within.

- REPORTING INFORMATION SECURITY WEAKNESSES
  Forterro has a responsible disclosure program with guidance on how to submit a discovery.

- ASSESSMENT OF AND DECISION ON INFORMATION SECURITY EVENTS
  Forterro has a procedure for assessing an incident and determining its severity and who needs to be informed at each level.

- RESPONSE TO INFORMATION SECURITY INCIDENTS
  Forterro has documented procedures and runbooks for responding to a security incident.

- LEARNING FROM INCIDENTS
  Forterro operates a post incident review process where a root cause analysis is carried out followed by a lessons learned review with recommendations and evaluated processes updated where appropriate.

- COLLECTION OF EVIDENCE
  Forensic capture of information on corporate systems is automatically stored in the SIEM service.

Business continuity – Information security aspects

- PLANNING INFORMATION SECURITY CONTINUITY
  The Forterro products are hosted in an AWS service in the Paris Region of France on a Cluster replicated to a further 2 datacentres with daily backups and hourly snapshots in a 6-hour rolling collection.

- IMPLEMENTING INFORMATION SECURITY CONTINUITY
  The Forterro Cloud ERP Service has documented processes and procedures that are regularly reviewed.

- VERIFY, REVIEW AND EVALUATE INFORMATION SECURITY CONTINUITY
  The information security continuity controls are reviewed at regular intervals to ensure that they are valid and effective during adverse situations.

Redundancies

- AVAILABILITY OF INFORMATION PROCESSING FACILITIES
  There is resilience built into each of the datacentre locations for power, cooling, network and individual component failure.