GDPR - DATA PROTECTION POLICY

7th September 2025

FSS GROUP

Est 2006

Field Support Services Group Ltd
Company Registration: 10202947
VAT: 329 6435 79
NCAGE: U1P58
DUNS: 2218833136

44 Bridge Street
Hereford HR4 9DG
United Kingdom

Tel +44 1432 850019
email: hereford@fss-gp.com
web: www.fss-gp.com

Table of Contents

INTRODUCTION

This Data Protection Policy is the overarching policy for data security and protection for the Field Support Services Group (hereafter referred to as “Field Support Services Group”, "us", "we", or "our").

This privacy policy ("policy") will help you understand how Field Support Services Group, uses and protects the data you provide to us.

We reserve the right to change this policy at any given time, of which you will be promptly updated.

Purpose

Supporting the 10 Data Security Standards, the General Data Protection Regulation (2016), the Data Protection Act (2018), the common law duty of confidentiality, and all other pertinent national legislations is the aim of the data protection policy. We embrace the concepts of data protection by design and by default and acknowledge data protection as a fundamental right.

This policy covers:

Our dedication to common law and legal compliance, as well as our data protection principles;

Protocols for both default and design-based data protection.

What User Data We Collect

When you visit our webpage, we may collect the following data:

- Your contact information and email address.
- Information relating to contracted services.
- Data profile regarding your online behaviour on our webpage.

Why We Collect Data

We are collecting your data for several reasons:

- To facilitate contracted service provisions and understand your needs.
- To improve our services and products.

Legal Basis for Processing Personal Data (GDPR)

We process your personal data based on the following legal grounds:

- Your consent, which you may withdraw at any time.
- The necessity for the performance of a contract with you.
- Compliance with a legal obligation.

Scope

This policy covers all of the data that we process, whether it be digital or hard copy, including special kinds of data.

All employees, including contract workers and temporary employees, are subject to this policy.

GDPR COMPLIANCE AND RECORDS OF PROCESSING

In our capacity as a data processor, we maintain detailed records of all processing activities. These records are updated regularly and are available to our clients (the data controllers) as required by our data processing agreements and upon request. The records include key information as mandated by Article 30, such as:

- The name and contact details of our organization and, where applicable, our representatives.
- The name and contact details of each data controller on whose behalf we are acting.
- A comprehensive list of the categories of processing activities carried out for each data controller.
- Details regarding data transfers to third countries or international organizations, if applicable.
- A general description of our technical and organizational security measures.

Defined Processing Activities

The processing activities we perform are strictly on behalf of and according to the documented instructions of our data controllers. Our services involve processing personal data to fulfil our contractual obligations in providing field support services. These activities include, but are not limited to, the following:

- **Secure Transport and Logistics:** We process personal data such as names, addresses, and flight details to manage secure airport transfers and ground transportation. This includes scheduling, dispatching, and providing real-time tracking services for secure travel.

- **Secure Communications and Coordination:** We process contact information and other necessary details to facilitate secure communication and coordination between the client, our field personnel, and local support teams to ensure efficient and safe operations.

- **Project and On-Site Support:** This involves the processing of personal data for the purpose of managing on-site personnel and logistics. This may include processing names, emergency contact information, and other relevant details to provide life support and project coordination.

- **Medical and Emergency Response:** In situations requiring medical support or emergency response, we may process special categories of data, such as health information, to ensure the well-being and safety of individuals. This processing is always done in a sensitive, secure manner and only as directed by the data controller.

- **Risk Management and Assessments:** We may process location data and other personal details to conduct security assessments and provide intelligence monitoring in high-risk environments. The purpose is to identify and mitigate threats to personnel and assets.

Principles

We will be open and honest about the care and treatment of service users and those who are lawfully acting on their behalf.

We will establish and uphold policies to guarantee adherence to the Human Rights Act of 1998, the Data Protection Act of 2018, the General Data Protection Regulation, the common law duty of confidentiality, and any additional relevant legislations.

All applicable regulations and public consent will be taken into consideration as we create and uphold policies for the appropriate and controlled sharing of staff and service user data with other parties.

In cases where consent is required for the processing of personal data, we will make sure that informed and explicit consent is acquired and recorded in an appropriate format and in easily comprehensible language. The person has been informed of the procedures to withdraw consent. Withdrawal of Consent procedures, and they can do so at any time. We guarantee that withdrawing consent is as simple as giving it.

We will undertake / commission annual audits of our compliance with legal requirements.

We acknowledge our accountability in ensuring that personal data shall be:

- Processed in a clear, equitable, and legal way;
- Collected for specified, explicit and legitimate reasons and not further processed in a manner that is incompatible with those goals;
- Adequate, relevant, and kept to a minimum given the objectives for which they are processed (also known as "data minimisation");
- Accurate and continuously updated;
- Stored for a period of time that allows data subjects to be identified for no longer than is required for the purposes for which the personal data are processed (a practice known as "storage limitation");
- Processed in a way that guarantees the personal data is appropriately secured.

We uphold the personal data rights outlined in the GDPR:

- The right to be informed;
- The right of access;
- The right to be corrected;
- The right to deletion;
- The right to limit processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling.

- Due to our size, we have determined that we are not required to have a Data Protection Officer (DPO), as we do not process special categories of data on a large scale.
- Nonetheless, to ensure that every individual's data rights are respected and that there are the highest levels of data security and protection in our organisation, we have appointed a member of staff to be our Data Security and Protection Lead. The Data Security and Protection Lead will report to the highest management level of the organisation.
- We will support the Data Security and Protection Lead with the necessary resources to carry out their tasks and ensure that they can maintain expertise.

SAFEGUARDING AND SECURING THE DATA

Field Support Services Group is committed to securing your data and keeping it confidential. Field Support Services Group has done all in its power to prevent data theft, unauthorized access, and disclosure by implementing the latest technologies and software, which help us safeguard all the information we collect online.

Our Cookie Policy

Please note that cookies don't allow us to gain control of your computer in any way. They are strictly used to monitor which pages you find useful and which you do not so that we can provide a better experience for you.

If you want to disable cookies, you can do it by accessing the settings of your internet browser. You can visit https://www.internetcookies.com, which contains comprehensive information on how to do this on a wide variety of browsers and devices.

Data Protection By Design And By Default

We shall implement appropriate organisational and technical measures to uphold the principles outlined above. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.

- We shall uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.
- It is unlikely that any small organisation will be required to undertake a data protection impact assessment. Though it is considered best practice to do one for your care plans at a minimum. Prior to starting any new data processing, we will assess whether we should complete a Data Protection Impact Assessment (DPIA).
- All new systems used for data processing will have data protection built in from the beginning of the system change.
- We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.
- In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.
- Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our staff and those we support.

OUR RESPONSIBILITIES

Our designated Data Security and Protection Lead is The Administrative Manager. The key responsibilities of the lead are:

- To ensure the rights of individuals in terms of their personal data are upheld in all instances and that data collection, sharing and storage is in line with the Caldicott Principles;
- To define our data protection policy and procedures and all related policies, procedures and processes and to ensure that sufficient resources are provided to support the policy requirements.
- To monitor information handling to ensure compliance with law, guidance and the organisation’s procedures and liaising with senior management to fulfil this work.

DATA PROTECTION PROCEDURES

Data Back Ups

Field Support Service Group conducts data back ups regularly. When using external storage devices, these are encrypted and locked in secure filing cabinets when not in use. Back-ups are not connected to any live data source.

Strong Passwords And Multi-Factor Authentication

Field Support Service Group use strong passwords on smartphones, laptops, tablets, email accounts and any other devices or accounts where personal information is stored.

Where possible, multi-factor authentication is used. Multi-factor authentication is a security measure to make sure the right person is accessing the data. It requires at least two separate forms of identification before access is granted. For example, you use a password and a one-time code which is sent by text message.

Filtering Suspicious Emails

FSS training and induction includes how to spot suspicious emails. Team members are trained to look out for signs such as bad grammar, demands for you to act urgently and requests for payment. New technologies mean that email attacks are becoming more sophisticated.

Anti-Virus And Malware Protection

Anti-virus software can help protect devices against malware sent through a phishing attack. All Field Support Services Group devices yare secured with the latest software.

Protecting devices when unattended

Field Support Service Group training and induction includes advice on securing devices - Lock your screen when you're temporarily away from your desk to prevent someone else accessing your computer. If you do need to leave your device for longer and at the end of each working day put it in a secure locked cabinet.

Wi-Fi connection is secure

Using public Wi-Fi, or an insecure connection, could put personal data at risk. Field Support Services Group use a secure connection in its offices when connecting to the internet. If using a public network, staff are advised to use a secure Virtual Private Network (VPN).

Limit access to those who need it

Different employees use different types of information. Field Support Services Group has implemented access controls to make sure people can only see the information they need. For example, payroll or HR may need to see workers' personal information, but operations staff do not.

If an employee leaves the company, or are absent for a long period of time due to sickness etc, Field Support Services Group will suspend their access to company systems.

Minimising Data Storage

Regularly removing data that is no longer required by the company reduces the amount of personal information at risk in the event of a cyber-attack or personal data breach.

Dispose of old IT equipment and records securely

Field Support Services Group ensures no personal data is left on computers, laptops, smartphones or any other devices, before professionally disposing of them. The company uses deletion software and contracted specialists to fully remove stored data.

DATA PROTECTION COMPLIANCE STATEMENT

In addition to maintaining comprehensive records of processing activities, the Field Support Services Group has implemented a robust data protection framework to ensure full compliance with the GDPR and all other applicable data protection legislation. Our commitment is to the secure, confidential, and responsible handling of all personal data on behalf of our data controllers.

Key Measures for Data Security and Privacy

1. **Data Processing Agreements (DPAs):** We do not commence any processing activities without a formal, written Data Processing Agreement (DPA) in place with the relevant data controller. These legally binding agreements explicitly define the scope, purpose, duration, and legal basis of all processing activities. They also outline our roles and responsibilities as a data processor, ensuring that personal data is handled only on documented instructions from the controller.

2. Technical and Organizational Measures: We have implemented a comprehensive suite of technical and organizational measures to ensure the security and integrity of the data we process. These measures include:

- **Access Controls:** Strict access controls and a principle of least privilege are applied to all data, ensuring that only authorized personnel can access personal data on a need-to-know basis.

- **Encryption:** Data is encrypted both in transit (using secure protocols like TLS) and at rest (using industry-standard encryption algorithms).
- **Confidentiality:** All personnel are bound by confidentiality agreements and receive regular training on data protection principles, security protocols, and their specific responsibilities under the GDPR.
- **Sub-Processors:** We maintain a rigorous vetting process for any sub-processors we engage. We only use sub-processors that provide sufficient guarantees of compliance with GDPR and, where applicable, are bound by the same data protection obligations as our group.

3. Data Subject Rights: As a data processor, we have established clear procedures to assist our data controllers in fulfilling their obligations to data subjects. This includes supporting controllers in responding to requests to exercise data subject rights, such as:

- The right to access personal data.
- The right to rectification of inaccurate data.
- The right to erasure ("right to be forgotten").
- The right to restriction of processing.
- The right to data portability.

4. Breach Notification Protocol: We have a well-defined protocol for the handling of personal data breaches. In the event of a security incident, our procedure ensures that we notify the data controller without undue delay after becoming aware of the breach. This allows the data controller to fulfill their own reporting obligations to the relevant supervisory authorities and data subjects in a timely manner.

Continuous Improvement and Auditing

We treat data protection as an ongoing commitment, not a one-time task. We regularly review and update our data protection policies and procedures to align with evolving legal requirements and best practices. Our processes are subject to regular internal and external audits to ensure our security measures remain effective and our records of processing are accurate and up to date.

This proactive approach ensures that we can provide our clients with the confidence that their data processing needs are handled with the utmost care, diligence, and compliance.

DATA SUBJECT RIGHTS ASSISTANCE PROCEDURE

The Field Support Services Group is committed to providing prompt and comprehensive assistance to The Client to ensure all data subject rights requests are handled in a timely and compliant manner. Our procedures are designed to facilitate your fulfilment of these

requests, as the data controller, while ensuring the security and integrity of the data we process.

General Protocol for All Requests

Upon receiving a data subject rights request, The Client's designated contact will notify our team immediately via a secure communication channel. We will prioritize the request and initiate our internal handling procedure, ensuring a swift and coordinated response. Our team will acknowledge receipt of the request and provide regular updates on its progress.

Detailed Procedures by Right

Access

- **Procedure:** We will work with The Client to identify and locate all personal data we process on behalf of the data subject. We will provide this data in a structured, commonly used, and machine-readable format to facilitate your response to the data subject.
- **Timeline:** We will aim to provide the requested data within **five working days** of receiving a valid request from The Client.

Rectification

- **Procedure:** Upon receiving a request for rectification, we will promptly update or correct any inaccurate personal data we hold. We will also inform any relevant third parties to whom the data may have been disclosed, as instructed by The Client.
- **Timeline:** We will action the rectification request within **three working days** of receiving a valid request from The Client.

Erasure

- **Procedure:** Following a valid request for erasure, we will securely and permanently delete the data subject's personal data from all of our systems. We will provide The Client with a confirmation of the erasure once completed. Any backups or archives will also be marked for deletion according to our data retention policy.
- **Timeline:** We will complete the erasure process within **seven working days** of receiving a valid request from The Client.

Restriction

- **Procedure:** If a data subject requests a restriction on the processing of their data, we will immediately cease all processing activities for the specified data. We will store the data securely but will not use it for any purpose until the restriction is lifted, as instructed by The Client. We will also inform any third parties to whom the data has been disclosed about the restriction.

- **Timeline:** We will apply the restriction to the specified data within **one working day** of receiving a valid request from The Client.

Data Portability

- **Procedure:** We will provide the personal data of the data subject to The Client in a structured, commonly used, and machine-readable format. This will enable The Client to transmit the data to another controller without hindrance. If technically feasible, we can also transmit the data directly to the new controller upon The Client's instruction.
- **Timeline:** We will provide the data in the required format within **ten working days** of receiving a valid request from The Client.

DISCLOSURE OF PERSONAL DATA TO THIRD-COUNTRY AUTHORITIES

The Field Support Services Group recognizes its strict obligations under the General Data Protection Regulation (GDPR) to protect personal data. This policy outlines our procedure for handling requests for the disclosure of personal data by courts, tribunals, or administrative authorities in third countries (i.e., countries outside the European Economic Area).

Our fundamental principle is that we will not comply with any such request unless it has a valid legal basis under EU law. This approach is in strict adherence to GDPR Article 48, which specifies that a judgment or decision from a third country requiring data transfer is only enforceable if it is based on an international agreement, such as a Mutual Legal Assistance Treaty (MLAT), in force between the requesting country and the European Union or a relevant Member State.

1. Mandatory Notification of Client

Immediate and Prior Notification: As the data processor, the Field Support Services Group will **immediately notify the client** upon becoming aware of any request for personal data from a third-country authority. This notification will be made before any action is taken to disclose the data, unless expressly prohibited by law for a legitimate and exceptional reason, such as a criminal investigation under the terms of a valid international agreement. The notification will include all available details of the request, including the requesting authority, the nature of the request, the data requested, and any associated legal documentation.

2. Our Handling Procedure

Upon receiving a third-country request for data disclosure, the following multi-step procedure is immediately activated:

- **Step 1: Legal Assessment:** Our legal and data protection teams will conduct a rigorous assessment to determine the legal validity of the request under GDPR. We will verify whether the request is based on a legally binding international agreement as required by Article 48. We will also assess if there is a compelling legal obligation to comply under Union or Member State law.
- **Step 2: Refusal to Disclose:** If the request is not based on a valid international agreement or a compelling legal obligation, we will formally refuse to disclose the data. We will communicate this refusal to the requesting authority, citing our obligations under the GDPR.
- **Step 3: Challenging the Request:** Should the requesting authority seek to enforce the request, we are committed to challenging it through all appropriate legal means. This includes, where necessary, engaging legal counsel in the relevant jurisdiction to defend our position and protect The Client's data.
- **Step 4: Data Minimization:** If, after a thorough legal review, we determine that a disclosure is legally required under an international agreement, we will only disclose the minimum amount of personal data strictly necessary to fulfill the request. This is in line with the GDPR's data minimization principle.

3. Commentary

This robust policy ensures that we do not comply with any "unauthorized" or "extralegal" requests for personal data. It places the ultimate decision-making power in the hands of The Client as the data controller, while leveraging our legal and operational expertise to manage the complexities of such requests.

This collaborative and legally compliant framework provides a strong line of defense against third-country subpoenas and legal orders, ensuring that data is never transferred without a valid legal basis and the full knowledge of the data controller.

PERSONAL DATA BREACH NOTIFICATION POLICY AND PROCESS

The Field Support Services Group has a robust and proactive policy for the identification, handling, and notification of personal data breaches. Our primary obligation as a data processor is to promptly notify the data controller, The Client, of any breach that affects personal data we process on your behalf.

Our policy is aligned with Article 33 of the GDPR, ensuring that you receive the information you need to fulfill your own reporting obligations to the supervisory authority and affected data subjects.

Investigation And Mitigation Plan

The Field Support Services Group has a structured and tested plan for investigating and mitigating personal data breaches. This plan is designed to be activated immediately upon the detection of a potential security incident to ensure a rapid and effective response, minimizing harm and fulfilling our contractual and legal obligations.

Policies and Processes

Our data breach management framework is built on a clear, five-stage process:

1. Incident Identification: We have implemented a continuous monitoring system with multiple layers of security, including intrusion detection systems, access logs, and anomaly detection software. All personnel are trained to recognize and report security incidents, no matter how minor. This ensures that any potential breach is identified as quickly as possible.

2. Triage and Assessment: Upon detection of a potential security incident, a dedicated incident response team is immediately activated. The team's first priority is to contain the incident and assess whether it constitutes a personal data breach. This involves a rapid investigation to determine:

- Whether personal data has been compromised.
- The nature and scope of the breach (e.g., unauthorized access, loss, destruction).
- The categories of personal data affected.
- The number of data subjects potentially impacted.

3. Containment and Remediation: Our technical teams work to contain the breach to prevent further damage. This may involve isolating affected systems, revoking access credentials, and implementing technical fixes. We then take immediate steps to remediate the underlying vulnerability and restore affected systems to normal operation.

4. Notification to Client: Once the initial assessment confirms that a personal data breach has occurred, we move directly to notification. We will not wait for a full investigation to be completed before notifying you. Our notification will contain, at a minimum, the following information, as required by the GDPR:

- A description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects and personal data records concerned.
- The likely consequences of the breach.
- A description of the measures we have taken or propose to take to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.
- The name and contact details of our Data Protection Officer (DPO) or other relevant contact point where more information can be obtained.

5. Documentation and Post-Incident Review: Following the breach, we will conduct a detailed post-incident review to understand the root cause, evaluate the effectiveness of our response, and update our policies and security measures to prevent a recurrence. A full report of this review will be made available to The Client.

Timescales

Our commitment to a prompt response is reflected in our strict notification timescales:

- **Initial Notification:** We will notify The Client of a personal data breach without undue delay, and in any event, within **24 hours** of becoming aware of it. This initial communication will provide all known details at that time.
- **Further Information:** We will provide further information as it becomes available, ensuring you have a complete picture of the breach to assist you in meeting your own obligations, particularly the 72-hour reporting deadline to the supervisory authority.
- **Final Report:** A comprehensive final report on the breach and our remediation efforts will be provided within **20 working days** of the breach being contained.

This framework ensures that the client is always the first to know and is fully equipped to manage its responsibilities as the data controller.

Policies and Processes

Our investigation and mitigation process follows a systematic approach based on established incident response best practices:

1. Incident Triage and Analysis:

- **Initial Assessment:** The moment a potential incident is detected, our security operations center (SOC) conducts a rapid triage. They confirm whether the event is a true security incident and, if so, its potential to compromise personal data.
- **Impact Analysis:** The incident response team quickly analyzes the scale of the incident, including the systems affected, the nature of the compromised data, and the potential impact on data subjects. This analysis is crucial for determining the severity of the breach.

2. Containment:

- **Immediate Actions:** The highest priority is to contain the breach to prevent further damage. This involves isolating affected systems from the network, revoking compromised access credentials, and disabling services that may be exploited.
- **Long-Term Containment:** Once the immediate threat is contained, we implement more robust, long-term measures to secure the environment, such as patching vulnerabilities, reconfiguring firewalls, and deploying additional monitoring tools.

3. Eradication:

- **Root Cause Identification:** Our forensic analysts conduct a thorough investigation to identify the root cause of the breach. This may involve analyzing logs, system images, and network traffic.
- **Threat Removal:** The malicious actors or software are fully removed from our systems. This includes cleaning malware, removing unauthorized user accounts, and addressing any backdoors.

4. Recovery and Restoration:

- **System Restoration:** We restore affected systems from secure backups to ensure the integrity of the data and the functionality of our services.
- **Verification:** Following restoration, a full security audit is conducted to verify that the environment is clean, secure, and ready for normal operations. This includes a review of all changes made during the remediation process.

5. Post-Incident Activities:

- **Forensic Report:** We compile a comprehensive forensic report detailing the timeline of the incident, the root cause, the data affected, and the steps taken to mitigate it.
- **Lessons Learned:** Our team conducts a "lessons learned" review to identify areas for improvement in our security posture and incident response plan. This includes updating policies, enhancing training for staff, and investing in new technologies.

Communication and Notification

Throughout the entire process, we maintain an open and transparent line of communication with the client.

- **Immediate Notification:** As detailed in our breach notification policy, we will provide The Client with a notification of the breach **without undue delay**, and in any event, within **24 hours** of becoming aware of it.
- **Regular Updates:** We will provide regular updates as new information is uncovered during the investigation.
- **Final Report:** A final, detailed report on the investigation and mitigation efforts is provided to The Client once all actions are complete.

This systematic and documented approach ensures that every breach is handled with the utmost seriousness, minimizing risk and ensuring full transparency with our data controllers.

STAFF PRIVACY AND DATA PROTECTION TRAINING POLICY

The Field Support Services Group considers a well-informed and data privacy-aware workforce to be an essential component of our overall compliance framework. We have established a mandatory training program to ensure that all staff, particularly those with access to personal data, understand their obligations under the GDPR and other applicable data protection laws.

Training Requirements and Content

All staff members are required to complete a comprehensive data protection training program. The content of this training is tailored to different roles but universally covers the following key areas:

- **Core Data Protection Principles:** Understanding the seven principles of data protection as outlined in the GDPR: lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.
- **Roles and Responsibilities:** Clear definitions of the roles of a data controller (The Client) and a data processor (Field Support Services Group), and the specific responsibilities of each staff member in protecting personal data.
- **Data Subject Rights:** Procedures for handling and assisting with data subject rights requests, including the right to access, rectification, erasure, and data portability.
- **Personal Data Breach Protocol:** The process for identifying a potential data breach and the strict internal and external notification procedures. This includes understanding the urgency of reporting and the steps for containment and mitigation.
- **Secure Data Handling:** Best practices for handling personal data, including the use of encryption, secure data transmission methods, and avoiding the use of unapproved personal devices or software for work-related data processing.
- **Acceptable Use of Data:** Guidance on the appropriate use and sharing of data, with a focus on avoiding any unauthorized transfers or disclosures.

Training Frequency

To ensure that our staff's knowledge remains current and relevant, our training program is conducted on a regular, mandatory basis.

- **Initial Training:** All new hires must complete the full data protection training as part of their onboarding process before being granted access to any personal data.
- **Annual Refresher Training:** All staff members are required to complete a refresher training session at least once every **12 months**. This training reinforces key concepts, addresses any updates in data protection law, and covers new threats or best practices.

- **Ad-Hoc Training:** Additional training sessions are provided as needed to address specific risks or in response to significant changes in our internal processes, software, or legal regulations.

Our commitment to continuous education ensures that all personnel are equipped with the knowledge and skills necessary to protect personal data and maintain a strong security posture.

APPROVAL

This policy has been approved by the Field Support Services Group, Higer Management Team and will be reviewed at least annually.