Information Technology Policy

[Compliance with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011]

Company Name: **Alimento Agro Foods Private Limited**

Effective Date: **24-11-2025 (Version 1.0)**

Review Schedule: Annually (Next Review: 24-11-2026)

Contents

1. Purpose and Scope

Preamble and Scope: Commitment to Data Integrity and Compliance

This **Information Technology (IT) Security and Sensitive Personal Data or Information (SPDI) Compliance Policy** formally articulates and establishes the unwavering and paramount commitment of **Alimento Agro Foods Private Limited** (hereinafter referred to as "the Company" or "**GIMI GIMI**") to upholding the absolute highest standards of data privacy, security, confidentiality, and integrity across all its operations.

Recognizing its indispensable and crucial role as a **'data fiduciary'**—a trustee and custodian legally and ethically responsible for the secure processing, storage, and management of personal data entrusted to it—the Company has meticulously designed, developed, and formally adopted this comprehensive policy framework.

This policy serves as the foundational document, a declaration of intent, and a set of mandatory rules governing the entire lifecycle of data within the Company.

Legal and Regulatory Mandate

This policy is specifically architected to ensure complete, rigorous, and proactive adherence to the statutory, regulatory, and procedural requirements set forth by the Indian legal framework. This mandate includes, but is not limited to:

- The Information Technology Act, 2000: Governing the use of electronic communication and commerce and defining core concepts like "data" and "computer resources."
- The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (hereinafter collectively referred to as the "SPDI Rules"): These rules, in particular, form the bedrock of this policy, dictating the stringent security measures, consent requirements, and privacy practices required for handling Sensitive Personal Data or Information (SPDI).

By adopting this framework, the Company aims not only to meet the minimum legal thresholds but to exceed them, thereby instilling profound trust among its customers, employees, partners, and all stakeholders, and safeguarding the organization against operational and reputational risks associated with data breaches or non-compliance. This commitment extends to ensuring all third parties and vendors processing data on GIMI GIMI's behalf are also bound by equivalent security and privacy obligations

2. Sensitive Personal Data Identification

The primary purpose of this policy is to articulate and enforce the stringent protocols governing the entire lifecycle of Sensitive Personal Data or Information (SPDI) and other confidential data within the Company's custody. This includes, but is not limited to, the procedures for:

- Collection: Defining lawful and fair means of acquiring SPDI, ensuring explicit consent is obtained where mandated.
- Storage: Establishing robust, secure, and access-controlled repositories for all collected data.
- Processing: Outlining legitimate and necessary uses of the data, strictly limited to the purposes for which it was collected.
- Transfer: Specifying secure methods and regulatory prerequisites for the internal and cross-border transfer of data.
- Destruction/Disposal: Mandating timely and irretrievable erasure or anonymization of SPDI once its legal or business purpose has been fulfilled.
- This policy applies comprehensively to all SPDI and confidential information gathered, processed, and maintained by the Company concerning its diverse community of associated persons, including, but not limited to:
- Employees: Current, former, and prospective personnel.
- Vendors and Business Partners: All third-party service providers, suppliers, and contractors interacting with the Company.
- Stakeholders: Customers, shareholders, and any other individuals whose SPDI is handled by GIMI GIMI.

Classification of Sensitive Personal Data and Information (SPDI)

In strict adherence to the requirements outlined in Rule 3 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (referred to as the "SPDI Rules"), the Company formally categorizes the following types of personal data and information, which are mandatorily collected and processed during the candidate onboarding and employment lifecycle, as Sensitive Personal Data or Information (SPDI).

The classification ensures that appropriate, high-level security and privacy measures are applied to this data throughout its lifecycle, as mandated by law.

Categories of Sensitive Personal Data and Information (SPDI)

Personal Identification and Biometric Information:

This category encompasses legally significant identification documents and personal attributes necessary for identity verification, background checks, and official record-keeping.

- Government-Issued Photo ID: Photocopies or scanned images of the Aadhaar Card, Permanent Account Number (PAN) Card, Voter Identification Card, and/or Driving Licence.
- Travel and Nationality Documents: Copies of a valid Passport, including visa pages, where applicable, for foreign nationals or employees traveling internationally.
- Personal Photographs: Recent passport-sized photographs used for internal identification, employee badges, and official documents.
- Biometric Data (Where applicable): Any information related to the physical or physiological characteristics of an employee, such as fingerprints or facial recognition data, collected solely for secure access control and attendance management systems.

Financial and Economic Data:

This data is crucial for the establishment of employment contracts, payroll processing, and statutory compliance related to compensation and benefits.

- Bank Account Details: Full bank account numbers, International Financial System Code (IFSC) or SWIFT codes, and branch details.
- Verification of Account: Scanned copies of cancelled cheques or bank passbook front pages, used to validate account ownership for salary disbursement.
- Compensation and Benefits Records: Detailed records pertaining to gross and net salary, fixed and variable components, allowances, tax deductions (TDS), Provident Fund (PF) details, Gratuity, and other employee benefits.
- Investment Declarations: Data related to employee tax-saving investments and declarations under various sections of the Income Tax Act.

Professional, Educational, and Statutory Compliance History:

This information is necessary for verifying credentials, assessing professional suitability, and ensuring compliance with labor and taxation laws.

- Career Documentation: Comprehensive Resumes (Curriculum Vitae) detailing employment history, roles, and responsibilities.
- Academic Verification: Copies of all relevant degree certificates, diploma transcripts, and professional qualifications.
- Previous Employment Records: Official relieving letters, experience certificates, and non-disclosure agreements (NDAs) from former employers.
- Tax Compliance Documents: Prior employment tax documents, including Form 16s and detailed salary slips from previous employers, required for accurate tax computation.

Contact, Residential, and Emergency Information:

Essential data required for official communication, address verification, and critical response protocols.

- Proof of Residence: Copies of recent utility bills (electricity, water, gas, or landline phone bill) or Ration Cards, used for residential address verification.
- Personal Contact Information: Permanent and current residential addresses, personal mobile phone numbers, and personal email addresses.
- Emergency Contact Information: Names, relationship status, and contact numbers of individuals to be notified in the event of an employee emergency or medical incident.

3. Purpose Limitation and Scope of Data Collection

Data collection by the Company shall be strictly governed by the principle of Purpose Limitation. This means that personal data, including Sensitive Personal Data or Information (SPDI), must be collected solely for specified, explicit, and legitimate business purposes.

Permitted Purposes for Data Collection:

- Identity Verification and Access Control: Collecting identification documents (e.g., Aadhar, Passport) necessary to confirm the identity of employees, contractors, and other data subjects, and to grant appropriate access to company premises and systems.
- Payroll and Compensation Processing: Collecting financial information (e.g., bank account details, PAN/Tax ID) and personal identifiers necessary for accurate calculation, disbursement, and reporting of salaries, benefits, and statutory deductions.
- Statutory and Regulatory Compliance: Collecting data required to comply with all applicable central, state, and local laws, including but not limited to labor laws, tax regulations, insurance requirements, and corporate governance mandates. This includes data for provident fund, social security, and health insurance.
- Employee Administration and Management: Collecting necessary details for managing the employment relationship, performance management, training and development, and internal communication.

Strict Prohibition on Unnecessary Data Collection:

The collection of any personal information or SPDI that is not demonstrably aligned with the Company's lawful and necessary business needs is strictly prohibited. All data collection processes must undergo a review to ensure that the data being requested is essential for the intended, explicit purpose.

Consent Mandate for Sensitive Personal Data or Information (SPDI)

In strict adherence to regulatory requirements, specifically Rule 5 of the relevant data protection regulations (e.g., Information Technology (Reasonable Security

Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, as applicable), the Company mandates the following:

Requirement for Prior Explicit Consent:

The Company shall obtain prior, informed, and explicit consent from the data subject (employee, applicant, or other relevant individual) before the collection, storage, or processing of any Sensitive Personal Data or Information (SPDI).

Format of Consent:

This mandatory consent must be secured in an auditable and retrievable format, which includes:

- Written Consent: A physical document signed by the data subject.
- Digital/Electronic Consent: An equivalent electronic record, such as an authenticated digital signature, a recorded acceptance via a secure digital portal, or a clear and unambiguous opt-in mechanism (e.g., check-box) that is time-stamped and logged.

The consent form must clearly state the purpose(s) for which the SPDI is being collected and the intended recipients or categories of recipients (e.g., HR department, third-party payroll vendor).

Data Minimization Principle

The Company shall strictly adhere to the internationally recognized principle of Data Minimization throughout all data collection activities.

Restriction to 'Need-to-Know' Basis:

Data collection is strictly limited to the absolute minimum necessary to achieve the stated, explicit purpose. Employees or systems are permitted to collect and process only the personal data that is essential for them to

perform their specific, assigned duties. This is defined as a "need-to-know" basis.

G

Authorization for Non-Standard Requirements:

Any request for data collection that goes beyond the documented, standard requirements for a specific business process (e.g., collection of additional health information not required for standard insurance, or excessive personal history) is considered non-standard. Such collections are only permissible after obtaining specific, documented authorization from a designated Data Protection Officer (DPO) or senior management representative, who must confirm the legitimate business need and compliance with the Purpose Limitation principle. All non- standard data must be handled with heightened security protocols.

4. Data Security and Access Control Framework

The Company is committed to implementing and maintaining robust, reasonable security practices and procedures designed to protect Sensitive Personal Data or Information (SPDI), particularly employee records, against unauthorized access, disclosure, alteration, or destruction. This framework establishes the foundational controls for both the physical location and the logical systems storing SPDI.

4.1.Physical and Logical Security

The security posture for SPDI relies on a multi-layered approach encompassing physical environment controls, stringent system protection measures, and strict infrastructure isolation.

4.1.1. Physical Security and Storage

1. **Secure Storage Location:** All digital employee records, including SPDI, are exclusively archived on a high-security, encrypted internal hard drive. This storage device is physically located within the confines of the permanently secured and access-controlled cabin belonging to the Head of Human Resources (HR).
2. **Environmental Controls:** The location housing the storage drive is protected by 24/7 surveillance, biometric access control for entry, and fire suppression systems to mitigate environmental risks. All physical access logs are reviewed monthly by the IT Security team.

4.1.2. System Protection and Hardening

1. **Authentication Protocols:** The storage systems, as well as any workstations used to directly access the SPDI, are protected via complex password and multi-factor authentication (MFA) protocols. Passwords must adhere to a strict policy requiring a minimum of 12 characters, including a mix of uppercase letters, lowercase letters, numbers, and special characters, and must be changed every 60 days.

2. **Anti-Malware Defense:** Comprehensive, next-generation antivirus and anti-malware software is installed, centrally managed, and automatically updated on all relevant storage and access systems.
3. **Proactive Scanning:** Regular, automated malware and vulnerability scanning is performed on all SPDI storage volumes no less than weekly. Any detected threats or vulnerabilities are escalated immediately to the IT Security Manager for remediation within 24 hours.
4. **Data Encryption:** All SPDI, both when stored (at rest) and when transferred internally (in transit) between authorized systems, is protected using industry-standard, strong encryption algorithms (e.g., AES-256).

4.1.3. Infrastructure Isolation

1. **Proprietary Hardware Mandate:** Data storage is restricted exclusively to Company-owned and managed hardware infrastructure. This policy strictly prohibits the use of personal, unmanaged devices or any form of third-party cloud hosting services (e.g., public cloud providers) for the storage or processing of SPDI to maintain maximum control over the data environment.
2. **Network Segmentation:** The systems holding SPDI are placed on a segregated, highly restricted internal network segment (VLAN) with strict firewall rules that permit communication only with designated, authorized workstations and internal services.

4.2. Access Control and Monitoring

Access to SPDI is managed on the principle of least privilege—users are granted the minimum level of access necessary to perform their required duties.

4.2.1. Strict Personnel Access

1. **Restricted Access List (RAL):** Access to SPDI is strictly limited to an approved, named list of individuals, which includes:
    - The Head of Human Resources (Primary Custodian).

- One designated Senior Finance Officer (for payroll and statutory compliance purposes only).

2. **Formal Authorization:** Any request for access by personnel outside the RAL must be submitted in writing to the Head of HR and the IT Security Manager, and must be approved by both prior to temporary access being provisioned. Temporary access is automatically revoked after 48 hours unless explicitly re-authorized.

4.2.2. Auditing and Accountability

1. **Comprehensive Logging:** The IT department ensures that detailed access logs, recording all successful and failed attempts to view, modify, or delete SPDI, are continuously maintained and securely archived for a minimum of one year. This includes user ID, timestamp, file accessed, and action performed.

2. **Mandatory Quarterly Audit:** The IT department conducts mandatory quarterly audits of these access logs. The primary objective of the audit is to verify strict protocol adherence, identify any suspicious access patterns, and ensure that only individuals on the Restricted Access List are accessing the data. Any identified deviations are reported immediately to the Compliance Officer and the Head of HR.

3. **Annual Review:** The Restricted Access List is formally reviewed and re-approved by senior management on an annual basis to ensure all access privileges remain current and necessary.

5. Data Retention and Destruction Policy

This section outlines the organization's strict policy and procedures governing the retention, storage, and secure destruction of all data, with particular emphasis on Sensitive Personal Data or Information (SPDI), to ensure compliance with all applicable statutory and regulatory requirements.

5.1. Retention Period for SPDI

- **Principle of Minimisation:** SPDI shall be retained only for the duration that is strictly necessary to fulfil the purpose for which it was collected, specifically for the period an individual is formally employed by the organisation.
- **Statutory and Regulatory Mandates:** Notwithstanding the employment period, SPDI retention must comply with any minimum or maximum periods explicitly mandated by relevant statutory laws, regulations, and industry standards (e.g., tax records, payroll information, and health and safety documentation). Where a conflict exists, the longer retention period, as required by law, shall prevail.

5.2. Secure Disposal of Data

The organisation is committed to the secure, irreversible, and timely destruction of all data, especially SPDI, once its required retention period has expired.

- **Timing of Disposal:** Upon the formal termination of an employee's contract (including resignation, retirement, or dismissal), all associated personal data and SPDI held in digital and physical formats shall be securely and permanently deleted or destroyed within **2 years** of the termination date.
- **Digital Data Destruction:**
    - **Data Wiping:** All data residing on active storage media (e.g., servers, hard drives, cloud repositories, portable devices) must be securely overwritten using approved, industry-standard data sanitisation software (e.g., according to NIST SP 800-88 Guidelines for Media Sanitization) to render the data irrecoverable.

- **Media Destruction:** For end-of-life or failed electronic media that cannot be reliably wiped (e.g., hard drives, solid-state drives, backup tapes), physical destruction methods such as degaussing or pulverisation shall be used to ensure the data is inaccessible.

- **Physical Records Destruction:**
  - **Shredding Standard:** All physical documents containing SPDI, confidential, or sensitive information must be destroyed using **cross- cut shredders** which meet a minimum security level (e.g., DIN P-4 or higher) to prevent reconstruction.
  - **Secure Segregation:** Physical records awaiting destruction must be kept in locked, secure containers until the destruction process is carried out by authorised personnel.

5.3. Logging and Audit Trail

To ensure accountability and demonstrate regulatory compliance, all disposal activities must be rigorously documented.

- **Disposal Log:** A comprehensive log must be maintained for every instance of data destruction, detailing:
  - The type of data destroyed (e.g., employee files, backup tapes).
  - The volume of data or number of records destroyed.
  - The date and time of the destruction.
  - The method of destruction used (e.g., cross-cut shredding, software overwrite).
  - The identification of the individual(s) who authorised and performed the destruction.
- **Internal Review:** These disposal logs and the overall adherence to the Data Retention and Destruction Policy shall be subject to regular **internal audits** to verify compliance, effectiveness, and consistency of application across the organisation. Any deviations or identified risks will be immediately addressed.

6. Third-Party Disclosure and Transfer

This section outlines the Company's strict policy and mandatory procedures governing the disclosure and transfer of Sensitive Personal Data or Information (SPDI) to third parties, ensuring compliance with all relevant data protection laws and contractual obligations.

6.1.Confidentiality and Permitted Disclosure

1. **General Prohibition:** The Company maintains a stringent prohibition against the disclosure, transfer, or sharing of any SPDI to unauthorized third parties under any circumstances.
2. **Explicit Consent Requirement:** Any necessary disclosure of SPDI to a third party must be strictly limited in scope and must be preceded by obtaining explicit, informed, and unambiguous written consent from the individual to whom the SPDI pertains, clearly specifying the purpose of the disclosure and the nature of the information being shared.
3. **Legal and Regulatory Mandates:** The only exception to the explicit consent rule is when the disclosure is strictly required by a court order, a legally binding statutory obligation, or a directive from a competent regulatory authority. In such cases, the Legal Department must be consulted, and the disclosure must be limited to the minimum data necessary to comply with the legal requirement. All such disclosures must be documented, including the legal basis and the specific data disclosed.

6.2. Vendor and Service Provider Compliance Management

1. **Designated Third-Party Vendor:** The Company has engaged **Pioneer HR Solutions Pvt Ltd** to manage and execute specific statutory compliance functions, which necessitate the processing of certain SPDI.
2. **Service Agreement and Data Processing Terms:** This engagement is formally documented and governed by a comprehensive service agreement (or Data Processing Agreement - DPA) which includes rigorous terms and conditions dedicated to data protection and confidentiality.

3. **Mandatory Contractual Safeguards:** The agreement with the vendor explicitly mandates:
    - Adherence to the Company's security standards and all applicable data protection laws.
    - The implementation of appropriate technical and organizational measures to protect the integrity and confidentiality of the SPDI.
    - Strict limitations on the vendor's use of the SPDI solely for the contracted purpose.
    - A defined procedure for the immediate notification and reporting of any security incident or breach.
4. **Liability and Indemnification:** The service agreement establishes clear provisions for **liability** and **indemnification** on the part of Pioneer HR Solutions Pvt Ltd in the event of a **third-party breach** originating within their systems or processes, including financial liability for any resulting damages, penalties, or losses incurred by the Company or the affected individuals.
5. **Audit and Monitoring Rights:** The Company retains the contractual right to periodically audit and monitor the vendor's compliance with the agreed- upon security and confidentiality standards.

6.3. Employee Obligations and Data Retention

1. **Non-Disclosure Clauses (NDAs):** All formal appointment letters and employment contracts include comprehensive and strict **non-disclosure clauses (NDAs)**. These clauses legally bind all employees to maintain the confidentiality of all Company data, including SPDI, both during and after the term of their employment.
2. **Mandatory Data Return and Device Surrender:** Upon an employee's exit from the Company (whether voluntary or involuntary), the employee is under a mandatory and explicit obligation to:
    - Immediately **return all physical and electronic documents**, records, and materials containing SPDI.

- **Surrender all Company-owned devices** (laptops, mobile phones, storage devices, etc.) used for work purposes to ensure all SPDI is secured and removed.
- Provide a written declaration confirming compliance with the data return requirements.

3. **Post-Termination Obligation:** The confidentiality and non-disclosure obligations survive the termination of employment and remain enforceable indefinitely or for the term specified in the NDA. Any breach of these obligations is subject to disciplinary action, legal remedies, and potential criminal prosecution.

7. Grievance Redressal Mechanism

7.1. Appointment of Grievance Officer and Compliance

In strict adherence to the requirements set forth in Rule 5(9) of the Information
Technology (Reasonable Security Practices and Procedures and Sensitive Personal
Data or Information) Rules, 2011 (referred to herein as the "SPDI Rules"), the Company has established a formal Grievance Redressal Mechanism. This mechanism is crucial for addressing any and all concerns, queries, or complaints related to data privacy, the processing of Sensitive Personal Data or Information (SPDI), and overall compliance with this IT Security and SPDI Policy. The appointment of a dedicated Grievance Officer is a mandatory step to ensure accountability and a structured approach to managing data subject requests and grievances.

7.2. Details of the Designated Grievance Officer

The Company has designated the following individual to serve as the Grievance Officer, responsible for overseeing the redressal process and ensuring timely resolution of all grievances:

Attribute	Detail
Grievance Officer Name	Mr. Shubham Choubey
Designation	Head – Logistics
Official Email Address	shubhamchoubey@mealofthemoment.com

Note: The Grievance Officer's contact details, especially the official email ID, will be prominently displayed on the Company's official website and internal portals to ensure easy access for all employees and relevant stakeholders.

1G

7.3. Service Standards for Grievance Redressal

The Company is committed to a transparent, efficient, and time-bound process for handling all grievances and requests submitted to the Grievance Officer. The following service standards are strictly adhered to:

- **Acknowledgment of Receipt:** The Grievance Officer, or their authorized delegate, shall formally acknowledge the receipt of any written request, complaint, or formal communication (including emails) **within 7 business days** of receiving the same. This acknowledgment will inform the complainant that their matter has been noted and is under review.
- **Resolution Timeline:** The Grievance Officer shall make all reasonable efforts to resolve the grievance, address the request, or provide a substantive response and final decision **within 30 calendar days** from the date of receipt of the complaint/request. If a resolution requires more time due to complexity or required investigation, the complainant will be notified of the delay and the expected new timeline.

7.4. Procedure for Submitting Grievances and Requests

Employees, data subjects, or authorized third parties may formally submit requests or complaints related to their personal data, SPDI, or this policy by following the procedure outlined below:

1. **Method of Communication:** All formal requests, complaints, or notifications must be submitted in writing **via email** to the official email address of the Grievance Officer specified above.
2. **Scope of Requests:** This mechanism is the formal channel for:
    - Formally requesting the **withdrawal of consent** for the collection, storage, processing, or use of their Sensitive Personal Data or Information (SPDI).

- Requesting **data correction, modification, or updating** of any inaccurate or incomplete SPDI held by the Company.
- Filing a formal **complaint** regarding any alleged breach of this IT Security and SPDI Compliance Policy or the provisions of the SPDI Rules.

3. **Required Information:** The communication must clearly state the nature of the request/complaint, the name and contact details of the person making the submission, and sufficient details to allow the Grievance Officer to identify the relevant data or incident. Anonymous complaints may be reviewed at the Company's discretion but may impede the ability to provide a formal resolution.

8. Audit and Governance Framework for SPDI Compliance

To maintain robust security posture and ensure continuous adherence to all regulatory and internal requirements concerning the protection of Sensitive Personal Data or Information (SPDI), the Company mandates a comprehensive Audit and Governance framework, which includes, but is not limited to, the following activities:

8.1 Annual Security and Compliance Audits:

- **Scope:** A formal, in-depth review of all systems, databases, and infrastructure components that store, process, or transmit SPDI. This includes application layer security, network perimeter defenses, cloud service configurations, and physical access controls.
- **Frequency:** Conducted once per year (annually), typically in the first quarter.
- **Reporting:** A detailed audit report, including identified vulnerabilities, risk ratings, and recommended remediation steps, must be submitted to the IT Security Committee and the Head of Governance.

8.2 Unscheduled and Scheduled Spot Checks:

a. **Purpose:** To verify operational security practices and ensure continuous vigilance.

b. **Password Hygiene Verification:** Regular, often unannounced, checks to verify adherence to the Company's complex password policy, multi-factor authentication (MFA) enforcement, and timely password rotation across all user accounts, especially those with privileged access to SPDI systems.

c. **Access Log and Activity Monitoring:** Routine verification and review of access logs, system activity, and privilege escalation attempts to detect and deter unauthorized access or anomalous behavior. Discrepancies must be investigated immediately.

8.3 Mandatory Cybersecurity Training and Compliance Modules:

d. **Half-Yearly Cybersecurity Training:** All staff members, regardless of their direct interaction with SPDI, must participate in half yearly interactive training sessions covering emerging cyber threats (e.g., phishing, ransomware), secure coding practices (for developers), and best practices for data handling.

e. **Annual SPDI Compliance Modules:** Specific, mandatory annual training focused on the legal, regulatory (e.g., GDPR, CCPA, local data protection laws), and internal policy requirements for handling and protecting SPDI. Successful completion, demonstrated by a passing score on a module-ending assessment, is mandatory for continued employment.

8.4 Comprehensive Incident Management and Remediation Protocol:

f. **Immediate Escalation:** Any suspected or confirmed security breach, data leak, or system compromise involving SPDI must be immediately escalated to the designated Incident Response Team, which includes the HR Head (for personnel-related data and communication) and the IT Administrator/Security Officer (for technical containment).

g. **Containment and Eradication:** A defined protocol must be followed for isolating affected systems, eradicating the threat, and restoring services securely.

h. **Corrective Action Logging:** All incidents, including the root cause analysis, the steps taken for containment and eradication, and the subsequent preventative measures (corrective actions), must be thoroughly documented in a central Incident Log for review by the Governance team to prevent future occurrences.