INFORMATION SECURITY MANAGEMENT SYSTEM POLICY V1.1

Table of Contents

INFORMATION SECURITY MANAGEMENT SYSTEM POLICY 5
Information Security Commitment 5
Scope of the Policy 5
Data Collection and Privacy 5
1. Data Classification and Handling 6
1.1. Sensitive Information and Classification Definitions 6
1.2. Handling Guidelines 6
1.3. Asset Identification and Risk Management 6
1.4. Our risk management framework involves 7
2. Detailed Security Controls and Procedures 7
2.1. Acceptable Use 7
2.2. Identity Management and Access Control 7
2.3. Individual Accounts: 7
2.3.1. Privileged Access Management: 7
2.3.2. Two-Factor Authentication (2FA): 8
2.3.3. Controlled Access to One-Time Passcodes (OTPs): 8
2.4. Mitigation of Malicious Activities: 8
2.4.1. Monitoring and Alerts: 8
2.4.2. Incident Response: 8
2.5. Role-Based Access Control (RBAC): 8
2.5.1. Regular Access Reviews: 9
● Employee Training and Awareness: 9
● Ongoing Education: 9
2.6. Activity Logs: 9
2.7. Compliance with Regulations: 9
2.8. Continuous Improvement: 9
2.8.1. Penetration Testing: 10
2.8.2. Protection Against Malware 10
2.8.3. Regular System Updates 10
2.8.4. Restricted Use of Company Assets 10
2.9. Remote Working 10

2.10. Physical Security 10
2.11. Backup 11
2.12. Cryptography & Key Management 11
2.13. Clear Desk and Clear Screen 11
2.14. Information Classification, Labelling, and Handling 11
2.15. Supplier Relationships 11
2.16. Secure Development 12
3.1. Role of the DevOps Team: Threat Monitoring and Detection: 12
3.2. Incident Documentation: 12
3.18. Reporting, Concerns, and Incident Handling 16
3.19. Regulatory Compliance: 16
3.20. Risk Management: 17
4. Cloud Services Security, Strategy and Implementation: 17
Management of Security Risks for AWs-hosted systems 17
4.1. Management of Information Security Risks for Third-Party API Suppliers 18
4.1.1. Supplier Risk Assessment 18
4.1.2. Due Diligence 18
4.1.3. Technical Integration Controls: 18
4.2. AWS Services in Use 19
4.2.1. Amazon EC2 (Elastic Compute Cloud): 19
4.2.2. Amazon S3 (Simple Storage Service): 19
4.2.3. Amazon RDS (Relational Database Service): 19
4.2.4. Amazon Route 53: 19
4.3. Google Cloud Services in Use 19
4.3.1. Gemini 19
4.3.2. Vertex AI 20
4.4. Data Backup and Redundancy 20
4.5. Strategic Considerations 20
4.6. Future Opportunities 20
5. Technological Controls 21
5.1. Access to Source Code: Policy and Safeguards 21
5.2. Key Policies and Practices 21
6. Resource Management Policy 22
7. Capacity Management 22
8. Management of Technical Vulnerabilities 22
8.1. Configuration Management 23

8.2. Two-Factor Authentication (2FA): 23
8.3. Strong Password Policies: 23
8.4. Privileged Access Management (PAM): 23
8.5. Information Deletion 23
8.6. Clock Synchronization 24
8.7. New Systems or Tools 24
8.8. Use of Privileged Utility Programs 24
8.9. Installation of Software on Operational Systems 24
8.10. Internal Portal and Telemetry Data: 25
8.11. Daily Reviews by DevOps Security Engineer: 25
A dedicated DevOps security engineer reviews this data daily to identify any unauthorised installations or changes. Prompt action is taken to address any anomalies, ensuring the integrity and security of operational systems. 25
8.12. Network Security and Application Security 25
8.13. Periodic Policy Reviews 25
8.14. Implementation of Security Measures: 25
8.15. Secure Development Life Cycle (SDLC) 25
● Secure Design & Architecture 25
● Code Reviews & Secure Coding 25
● Automated & Manual Testing 26
● Continuous Integration & Deployment (CI/CD) 26
● Environment Segregation 26
We maintain separate and isolated infrastructure clusters for different clients, ensuring data segregation, minimising cross-tenant risks, and enhancing overall system security. 26
● Compliance & Governance: 26
8.20. Management Review: 26
8.21. Deployment 26
8.22. Alignment with Application Security Policy: 26
9. Privacy and Protection of Personally Identifiable Information (PII) 27
Identification of Requirements 27
Documented Policies and Procedures 27
Implementation of Controls 27
Monitoring and Continuous Improvement 27
Conclusion and Statement of Policy 28

INFORMATION SECURITY MANAGEMENT SYSTEM POLICY

This Policy serves as the definitive statement of EarnFlex's commitment to protecting its data and technology infrastructure, ensuring that every employee, contractor, and business partner upholds our stringent security and privacy standards. EarnFlex Ltd maintains a robust Information Security Management System (ISMS) and Cyber Security Policy designed to safeguard our data, technology infrastructure, and reputation. This Policy provides clear guidance for preserving the confidentiality, integrity, and availability of all information assets—including data from customers, business partners, investors, and staff—by detailing required standards of conduct, risk management practices, and security controls. It is expected that every employee and external partner adheres strictly to this Policy, as any deviation could cause severe financial damage or reputational harm to the Company.

Information Security Commitment

EarnFlex's senior management unequivocally commits to:

- Allocating necessary resources to implement and continuously improve the ISMS.
- Integrating security objectives into our overall business strategy.
- Ensuring compliance with all applicable legal, regulatory, and statutory requirements.
- Promoting a culture of security awareness where every action reflects our commitment to safeguarding sensitive information.

Any insensitivity to these principles or failure to follow this Policy will be considered a serious breach of trust, subject to strict disciplinary measures.

Scope of the Policy

This Policy applies to all employees, contractors, and any person with permanent or temporary access to EarnFlex's systems and hardware. Our ISMS scope encompasses:

- Flexible Staffing Platform, Facilitating secure connections between employers and pre-vetted workers,
- Compliance Software as a Service (SaaS): Delivering software solutions that help clients meet regulatory requirements,
- Supporting Infrastructure: All IT systems, applications, networks, data storage facilities, and cloud-based services.
- Third-Party Relationships: Any vendor or partner that handles or accesses sensitive information on our behalf.

Data Collection and Privacy

- EarnFlex collects personal and confidential information only to the extent necessary for business operations. We obtain data directly from:
- Employees and Contractors: To assess suitability, support development, and manage working relationships.
- Customers: To provide essential services and ensure proper system delivery.
- Suppliers and Business Partners: To evaluate their offerings and manage business relationships.

At all times, we ensure that individuals understand the purposes of collection and how their data may be used or disclosed. Should an individual refuse to provide the required information, the consequences, including possible discontinuation of the relationship, will be explained.

1. Data Classification and Handling

1.1. Sensitive Information and Classification Definitions

All information is categorized into four classifications to ensure appropriate handling:

- Secret: Information whose unauthorized disclosure could cause serious financial, reputational, or regulatory damage. Examples: Profit forecasts, merger plans, Board meeting minutes.
- Confidential: Proprietary information accessible only to those with a need-to-know. Examples: New product plans, client contracts, audit findings.
- Internal Only: Information relating to internal operations that, while not highly sensitive, should remain within the organization. Examples: Organizational policies, and internal announcements.
- Unrestricted: Information approved for public release. Examples: Marketing materials, and publicly available website content.

1.2. Handling Guidelines

All data must be stored on company-managed devices or secure cloud services.

- Confidential data must be encrypted during storage and transmission.
- Hard copies and electronic media must be securely disposed of when no longer required.

For additional details, please refer to the EarnFlex Privacy Notices provided for employees and customers.

1.3. Asset Identification and Risk Management

EarnFlex maintains a comprehensive register of all critical information assets, including:

- Customer data, business intelligence, IT infrastructure, software applications, and communication systems.
- Employee and contractor records.

1.4. Our risk management framework involves

- Identification: Systematic cataloguing of assets and potential threats.
- Assessment: Regular analysis of vulnerabilities and impact on operations.
- Mitigation: Deployment of technical, administrative, and physical controls.
- Continuous Review: Regular updates and audits to address emerging risks.

2. Detailed Security Controls and Procedures

2.1. Acceptable Use

- Guidelines: All systems must be used for legitimate business purposes only. Unauthorized access, modification, or sharing of data is strictly prohibited.
- Monitoring: Internet, email, and system activity are regularly audited. Any deviation will be subject to investigation and disciplinary action.

2.2. Identity Management and Access Control

EarnFlex has implemented a robust Identity and Access Management (IAM) framework to ensure that only authorized individuals have access to sensitive systems, data, and resources. This framework is designed to prevent unauthorized access, mitigate malicious activities, and maintain the integrity of the company's digital environment. Below is an expanded explanation of the company's identity management practices:

- Unique Login Credentials:

2.3. Individual Accounts:

Each employee receives unique login credentials (username and password) to access company systems, ensuring clear accountability and traceability. Shared accounts are strictly prohibited to prevent tracking ambiguities and reduce credential misuse risks. Login IPs are monitored, and all data-altering activities are logged for every session.

2.3.1. Privileged Access Management:

Access to sensitive systems and resources is granted based on the Principle of Least Privilege (PoLP), meaning employees are given access only to the data and tools necessary for their specific roles. Privileged accounts (e.g., administrative access) are restricted to authorized personnel, such as IT administrators, team leads, and senior leadership.

Access rights are regularly reviewed and updated to reflect changes in roles or responsibilities.

2.3.2. Two-Factor Authentication (2FA):

Enhanced Security. To add an extra layer of security, EarnFlex has enabled Two-Factor Authentication (2FA) for all user accounts. This requires employees to provide two forms of identification to log in:

Something they know (e.g., a password).

Something they have (e.g., a one-time passcode sent to their registered device).

2.3.3. Controlled Access to One-Time Passcodes (OTPs):

The one-time passcode (OTP) is accessible only to team leads, line managers, and senior leadership. This ensures that OTPs are managed responsibly and reduces the risk of misuse.

In cases where an employee requires assistance (e.g., account recovery), the OTP can be generated by authorized personnel, who will verify the employee’s identity before providing access.

2.4. Mitigation of Malicious Activities:

Preventing Unauthorized Access: By requiring 2FA and restricting OTP access to trusted personnel, EarnFlex significantly reduces the risk of unauthorized access, even if login credentials are compromised.

2.4.1. Monitoring and Alerts:

The IAM system continuously monitors login attempts and user activity. Any suspicious behaviour, such as multiple failed login attempts or access from unrecognized devices or locations, triggers an alert for immediate investigation.

2.4.2. Incident Response:

If a potential security breach is detected, the Information Security Team immediately engages the CTO and DevOps team to assess the situation and initiate swift action. This may include locking affected accounts, revoking user access, containing impacted services, and performing detailed forensic investigations to determine the cause and scope of the breach.

2.5. Role-Based Access Control (RBAC):

Access Based on Roles. Access to systems and data is granted based on the employee's role within the organization. For example:

- Marketing Team: Access to marketing tools, social media accounts, and analytics platforms.
- Finance Team: Access to financial systems and sensitive accounting data.
- IT Team: Access to administrative tools and network configurations.

2.5.1. Regular Access Reviews:

Access permissions are reviewed periodically to ensure they remain aligned with the employee's current role and responsibilities. Any unnecessary access is revoked promptly.

- **Employee Training and Awareness:**

Security Best Practices: Employees are trained on the importance of safeguarding their login credentials and using 2FA effectively. This includes:

- Creating strong, unique passwords and changing them regularly.
- Avoiding the use of personal devices or unsecured networks for work purposes.
- Recognizing and reporting phishing attempts or suspicious activities.

- **Ongoing Education:**

Regular updates and reminders about identity management policies are shared with employees to reinforce security awareness.

Auditing and Compliance:

2.6. Activity Logs:

The IAM system maintains detailed logs of all user activities, including login attempts, access requests, and changes to permissions. These logs are regularly reviewed to detect and address any anomalies.

2.7. Compliance with Regulations:

The company's identity management practices are designed to comply with relevant data protection regulations, such as GDPR, HIPAA, or ISO 27001. This includes ensuring that access controls and authentication mechanisms meet regulatory standards.

2.8. Continuous Improvement:

EarnFlex regularly seeks feedback from employees and stakeholders to identify areas for improvement in the IAM framework.

Updates to the system are implemented to address emerging threats and incorporate new technologies.

2.8.1. Penetration Testing:

Periodic penetration testing is conducted to evaluate the effectiveness of the IAM system and identify potential vulnerabilities.

2.8.2. Protection Against Malware

To safeguard its systems and data, the company has implemented a multi-layered approach to malware protection:

2.8.3. Regular System Updates

The company ensures that all systems are periodically updated with the latest versions of firewalls and Microsoft Defender. These updates provide enhanced protection against emerging threats and vulnerabilities.

2.8.4. Restricted Use of Company Assets

Only company-approved assets are permitted for internal use, reducing the risk of malware introduction through unauthorised devices or software.

2.8.5. Employee Training

Employees are trained to recognise and respond to potential threats, such as phishing emails and suspicious websites. This training fosters a culture of vigilance and reduces the likelihood of malware infections caused by human error.

2.9. Remote Working

- Secure Connectivity: Remote access must be via secure VPNs with encryption.
- Device Management: Only company-approved devices with current antivirus and security patches may be used.
- Data Handling: Sensitive data must be accessed and stored only on secure, approved platforms.
- Training: Specific remote working security training is mandator

2.10. Physical Security

- Access Control: Entry to offices is controlled by a code entry system only authorised workers know the code and need to enter while entering the offices.
- Surveillance: CCTV and visitor logs monitor all sensitive areas.
- Asset Management: All IT equipment is recorded, maintained, and securely disposed of when obsolete.

2.11. Backup

- Frequency: Critical data is backed up daily using automated schedules.
- Encryption and Storage: All backups are encrypted and stored in multiple geographically diverse locations in the AWS Cloud.
- Testing: Regular restore tests ensure data integrity and effective disaster recovery.

2.12. Cryptography & Key Management

- Standards: Use of industry-standard encryption (e.g., AES-256, TLS 1.2+) for data in transit and at rest.
- Key Lifecycle: Secure generation, storage, periodic rotation, and eventual disposal of cryptographic keys using dedicated key management systems.
- Access Controls: Strict restrictions and auditing for any access to cryptographic materials.

2.13. Clear Desk and Clear Screen

- Policy: Employees must not leave sensitive information unattended on desks or screens.

- Enforcement: Workstations must be locked when unattended; physical documents must be secured or shredded.

2.14. Information Classification, Labelling, and Handling

- Framework: All information is classified as Secret, Confidential, Internal Only, or Unrestricted.
- Procedures: Documents and electronic files must be clearly labelled according to their classification and handled using secure methods (e.g., encryption, controlled sharing).

2.15. Supplier Relationships

- Due Diligence: All third-party vendors undergo rigorous security assessments.
- Contracts: Binding agreements specify data protection, security controls, and incident reporting requirements.
- Oversight: Regular audits and performance reviews ensure ongoing compliance.

2.16. Secure Development

- SDLC Integration: Security is embedded in every stage of the software development lifecycle.
- Testing: Regular code reviews, static and dynamic analyses, and penetration tests are required.
- Change Management: All development activities are governed by formal change management processes with documented risk assessments.

3. Threat Intelligence and Incident Management:

EarnFlex maintains a proactive approach to identifying, managing, and mitigating threats to its digital infrastructure and data. The DevOps team plays a central role in this process, working closely with the Information Security Team and senior leadership to ensure that all threats are addressed promptly and effectively. Below is a detailed explanation of the threat intelligence process, including roles, responsibilities, and continuous improvement strategies.

3.1. Role of the DevOps Team: Threat Monitoring and Detection:

The DevOps team is responsible for continuously monitoring the company's systems, networks, and applications for any signs of suspicious or malicious activity. This includes:

- Using advanced threat detection tools and software to identify potential threats in real-time.
- Analysing system logs, network traffic, and user activity to detect anomalies.
- Staying updated on the latest cybersecurity threats and vulnerabilities through threat intelligence feeds and industry reports.

3.2. Incident Documentation:

Every threat or attack, whether virtual or online, is thoroughly documented by the DevOps team. Documentation includes:

- The nature of the threat (e.g., malware, phishing, DDoS attack, unauthorized access).
- The date, time, and duration of the incident.
- The systems, applications, or data affected.
- The steps taken to detect, contain, and mitigate the threat.
- The impact of the incident on operations, data integrity, or customer trust.

3.3. Kill Time Measurement:

The DevOps team tracks the kill time for each threat, which refers to the time taken from the initial detection of the threat to its complete resolution. This metric is critical for evaluating the efficiency of the company's response mechanisms.

3.4. Senior Leadership Review:

The CTO (Chief Technology Officer) and CEO (Chief Executive Officer) periodically review all documented threat activities and the associated kill times. This review process ensures that senior leadership is fully informed about the company's security posture and can make strategic decisions to enhance protection.

3.5. Key Focus Areas During Review:

- The frequency and severity of threats.
- The effectiveness of the response strategies employed.
- Trends or patterns in threat activity that may indicate systemic vulnerabilities
- Areas where kill times can be reduced to minimize damage and downtime.

3.6. Development of New Strategies and Procedures:

Based on the insights gained from reviewing threat activities, EarnFlex develops and implements new strategies and procedures to strengthen its security framework. These may include:

- Enhanced Threat Detection Tools: Investing in advanced tools and technologies to improve the accuracy and speed of threat detection.
- Incident Response Plans: Updating and refining incident response protocols to ensure a swift and coordinated response to future threats.
- Employee Training: Conduct regular training sessions to educate employees about emerging threats and best practices for preventing security breaches.
- System Hardening: Implementing additional security measures, such as firewalls, intrusion detection systems, and encryption, to protect critical systems and data.
- Third-Party Audits: Engaging external cybersecurity experts to conduct audits and penetration testing to identify and address vulnerabilities.

3.7. Continuous Improvement:

EarnFlex is committed to a culture of continuous improvement in its threat intelligence and security practices. This involves:

- Regularly updating threat intelligence feeds and incorporating lessons learned from past incidents.
- Conducting post-incident reviews to identify gaps in the response process and implement corrective actions.
- Benchmarking against industry standards and best practices to ensure EarnFlex remains at the forefront of cybersecurity.

3.8. Communication and Transparency:

EarnFlex maintains open communication channels with all stakeholders, including employees, customers, and partners, regarding its threat intelligence efforts. This includes:

- Providing regular updates on the company’s security posture and any significant threats that have been mitigated.
- Sharing insights and best practices to help stakeholders protect their own data and systems.
- Ensuring transparency in the event of a major security incident, including timely notifications and clear explanations of the steps taken to resolve the issue.

3.9. Business Continuity & Disaster Recovery (BC/DR) Policy/Plan

- Planning: Detailed BC/DR plans outline Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for all critical systems.

- Redundancy: Implementation of redundant systems and failover mechanisms minimizes downtime.
- Testing: Regular drills and simulations ensure effective crisis response.
- Communication: A clear crisis communication plan informs stakeholders during disruptions.

3.10. Incident Management Procedure and Log

- Reporting: All incidents must be reported immediately via designated channels.
- Response: A structured incident response process (detection, containment, eradication, recovery, and post-incident analysis) is followed.
- Documentation: Detailed incident logs and reports support continuous improvement and compliance audits.

3.11. Change Management Procedure

- Process: All changes to IT systems, applications, and security controls require formal documentation, risk assessment, and approval.
- Testing: Changes are validated in controlled environments before full deployment.
- Communication: Affected stakeholders are promptly informed, with full documentation maintained for audit purposes.

3.12. Human Resource Security

- Screening: Comprehensive background checks are performed for new hires and contractors.
- Training: Mandatory security awareness training is provided at induction and periodically thereafter.
- Exit Procedures: Upon termination or resignation, all access rights are revoked, and Company assets are recovered.

3.13. Disciplinary Process

- Enforcement: Breaches of this Policy result in disciplinary measures, ranging from formal warnings to termination, in accordance with the severity of the offence.
- Investigation: Any alleged breach is thoroughly investigated, and corrective actions are implemented.
- Accountability: Managers and supervisors are held accountable for ensuring their teams adhere to the Policy.
- Appeals: A formal appeals process is available to ensure fairness and transparency in disciplinary actions.

3.14. Quality and Security of Data/ Information Transfer

EarnFlex ensures that all personal and confidential information is:

- Accurate and Up to Date: Collected, stored, and maintained to the highest standards.
- Transferred Securely: All data transfers are conducted using robust encryption protocols.
- Properly Disposed: When data is no longer required, it is securely destroyed using approved methods (e.g., shredding, secure wiping).

3.15. Removable Media Guidelines

The use of removable media is strictly controlled:

- Approval: Only permitted with a valid business case approved by Waqas Ahmed.
- Security: Removable media used for storing sensitive data must be encrypted (minimum AES-256) and be subject to strict inventory and disposal controls.
- Disposal: Obsolete or damaged removable media must be securely disposed of by certified suppliers.

3.16. Use of the Internet, Business Applications, and Telephones

All online and telecommunication resources are for business purposes only:

- Guidelines: Employees must not use these systems for activities that compromise security or violate legal obligations.
- Restrictions: Prohibited activities include accessing inappropriate content, sharing confidential data externally, and installing unauthorized software.
- Monitoring: Usage is subject to regular monitoring to ensure compliance.

3.17. Training and Awareness

EarnFlex is committed to continuous security education:

- Induction: All new staff receive comprehensive training on our ISMS, data privacy, and security practices.
- Ongoing Training: Regular cybersecurity training, phishing simulations, and periodic assessments may be conducted.
- Policy Reviews: Annual reviews and updates ensure that all employees remain current with evolving threats and best practices.

3.18. Reporting, Concerns, and Incident Handling

Any concerns, complaints, or suspected security breaches must be reported immediately:

- Reporting Channels: Reports should be directed to Daniel Looney

- Incident Handling: The designated Information Security Officer will investigate and address all incidents promptly, ensuring that remedial actions are taken and documented.

Information Security Plan for Incident Response and Project Management:
The integration of information security into project management is a critical aspect of ensuring that projects are delivered successfully while safeguarding sensitive data and complying with regulatory requirements. Each project management team is responsible for maintaining a structured approach to information security throughout the project lifecycle. Below is an expanded explanation of how information security is embedded into project management practices:

Scope of Work Documentation:
The project management team maintains a comprehensive Scope of Work (SOW) document that outlines the project's objectives, deliverables, timelines, and resources. This document serves as the foundation for aligning the project with information security requirements.
Security Considerations in Scope, the SOW must explicitly include information security considerations, such as:

- The types of data that will be handled during the project (e.g., personal data, financial information, intellectual property).
- The systems, tools, and platforms that will be used to manage and store project data.
- The potential risks associated with the project and the measures to mitigate them.

3.19. Regulatory Compliance:

Identification of Applicable Regulations: Depending on the project's nature, the team must identify and comply with relevant regulatory authorities and bodies, which are included in the legal register.

Compliance Integration: The project plan must incorporate steps to ensure compliance with these regulations, such as:

- Conducting a Data Protection Impact Assessment (DPIA) to identify and address privacy risks.
- Implementing encryption, access controls, and other security measures to protect sensitive data.
- Ensuring that third-party vendors or contractors involved in the project also comply with relevant regulations.

3.20. Risk Management:

- Risk Assessment: The project management team will conduct a thorough risk assessment to identify potential information security risks. This includes:
- Assessing the likelihood and impact of risks such as data breaches, unauthorized access, or system failures.
- Identifying vulnerabilities in the project's processes, tools, or technologies.

Risk Mitigation Plan: A risk mitigation plan must be developed and integrated into the project plan. This plan should include:

- Specific actions to reduce the likelihood or impact of identified risks.
- Contingency plans for responding to security incidents.
- Regular reviews and updates to the risk assessment as the project progresses.

4. Cloud Services Security, Strategy and Implementation:

The decision to select and implement cloud services platforms is a strategic one, typically driven by the CEO and CTO in collaboration with other key stakeholders. This decision-making process involves a thorough review of the organization's use cases, technical requirements, scalability needs, cost considerations, and long-term business goals. The choice of cloud platforms is critical, as it impacts the company's ability to innovate, maintain security, and scale operations efficiently.

Currently, EarnFlex has adopted a multi-cloud strategy, leveraging two major cloud service providers: **Amazon Web Services (AWS)** and **Google Cloud Platform (GCP)**. This approach allows the organization to take advantage of the unique strengths and capabilities of each platform while mitigating risks associated with vendor lock-in and ensuring redundancy.

Management of Security Risks for AWs-hosted systems

EarnFlex manages security risks associated with systems hosted on AWS through clearly defined and documented processes and procedures. These include conducting regular supplier risk assessments, enforcing strict access controls and encryption of data both in transit and at rest, and continuously monitoring infrastructure through logging and audit trails. EarnFlex also maintains formal incident response procedures to ensure timely detection, escalation, and management of security incidents involving AWS-hosted systems. Additionally, EarnFlex regularly reviews AWS's security posture and compliance documentation, verifying alignment with established security requirements and internal standards.

4.1. Management of Information Security Risks for Third-Party API Suppliers

EarnFlex Ltd implements a simplified, practical process tailored specifically for managing the information security risks associated with third-party API suppliers, particularly large-scale providers such as AWS, who typically provide comprehensive public documentation instead of filling out custom forms. The following outlines our straightforward approach:

4.1.1. Supplier Risk Assessment

Suppliers are classified (Low, Medium, High) based on:

- Nature and sensitivity of data accessed.
- Criticality to EarnFlex's business operations.
- Reputation and established certifications of the supplier.

4.1.2. Due Diligence

Verification of supplier security standards via publicly available certifications and security assurances, such as:

- ISO 27001 certification
- SOC 2 Type II reports
- GDPR compliance statements (where applicable)

4.1.3. Technical Integration Controls:

Secure integration using industry-standard practices:

- Secure authentication (API keys, OAuth, JWT).
- Mandatory encryption of data in transit (minimum TLS 1.2).
- Application of strict API permissions and controls (Principle of Least Privilege).

4.1.4. Incident Management

Clearly defined procedure for handling security incidents involving suppliers, including notification processes, internal escalation, and coordinated remediation actions.

4.2. AWS Services in Use

EarnFlex has integrated the below AWS services into its infrastructure, focusing on scalability, reliability, and data security. The key AWS services currently in use include:

4.2.1. Amazon EC2 (Elastic Compute Cloud):

EC2 provides scalable virtual servers, enabling EarnFlex to run applications and workloads with flexibility. The use of EC2 instances ensures that the organization can scale compute resources up or down based on demand, optimizing costs and performance.

4.2.2. Amazon S3 (Simple Storage Service):

S3 is used for secure, durable, and highly scalable object storage. EarnFlex relies on S3 buckets to store critical data, including backups, application data, and other assets. S3's robust data management features ensure data integrity and accessibility.

4.2.3. Amazon RDS (Relational Database Service):

RDS simplifies the management of relational databases, offering support for databases like MySQL, PostgreSQL, and others. EarnFlex uses RDS to maintain its structured data, ensuring high availability, automated backups, and seamless scalability.

4.2.4. Amazon Route 53:

Route 53 is a scalable domain name system (DNS) web service that ensures reliable routing of user requests to the company's applications. It also plays a role in data safeguarding by enabling health checks and failover configurations.

4.3. Google Cloud Services in Use

On the Google Cloud side, EarnFlex has adopted services that align with its needs for advanced analytics, machine learning, and AI-driven solutions. The primary GCP services in use include:

4.3.1. Gemini

Gemini is being utilized for specific use cases, likely related to data analytics, collaboration, or productivity. Its integration into the company's workflow enhances efficiency and supports data-driven decision-making.

4.3.2. Vertex AI

Vertex AI is Google Cloud's unified machine learning platform, which enables EarnFlex to build, deploy, and scale AI models more effectively. By leveraging Vertex AI, the organization can accelerate its AI initiatives, from model training to deployment, while maintaining a streamlined workflow.

4.4. Data Backup and Redundancy

EarnFlex maintains backups of critical data in **Amazon S3 servers to ensure data resilience and business continuity**. This approach provides an additional layer of security, ensuring that data is protected against loss or corruption, by storing backups in S3, EarnFlex benefits from AWS's robust infrastructure, which includes features like versioning, encryption, and cross-region replication.

4.5. Strategic Considerations

The decision to use both AWS and GCP reflects a strategic approach to cloud adoption. By leveraging the strengths of both platforms, EarnFlex can:

- Optimize costs by selecting the most cost-effective services for specific use cases.
- Enhance performance by using specialized tools from each provider (e.g., Vertex AI for machine learning on GCP and RDS for database management on AWS).
- Ensure redundancy and disaster recovery by maintaining backups across platforms.
- Avoid vendor lock-in, giving EarnFlex flexibility to adapt to future technological changes.

4.6. Future Opportunities

As EarnFlex continues to grow, there may be opportunities to expand its use of cloud services. For example:

- Exploring additional AWS services like Lambda for serverless computing or CloudFront for content delivery.
- Expanding GCP usage with services like Big Query for advanced data analytics or Cloud Spanner for globally distributed databases.
- Implementing hybrid or multi-cloud management tools to streamline operations across platforms.

In conclusion, the company's current cloud strategy, driven by the CEO and CTO, demonstrates a thoughtful and balanced approach to cloud adoption. By leveraging the strengths of AWS and GCP, the organization is well-positioned to meet its current needs while remaining agile for future growth and innovation.

5. Technological Controls

5.1. Access to Source Code: Policy and Safeguards

The company prioritizes the security and integrity of its source code, recognising it as a critical asset that requires robust protection. To ensure the safety of the source code, the company has implemented a comprehensive set of policies and procedures. These measures are designed to restrict access, monitor activities, and provide mechanisms to respond effectively to any potential breaches or unauthorised changes.

5.2. Key Policies and Practices

Restricted Access to Source Code

Access to the source code is strictly limited to authorised personnel only. This includes:

- DevOps Engineers: Individuals directly responsible for developing, maintaining, and deploying the code.

- CEO and CTO: Senior leadership with oversight responsibilities for the company’s technical operations and strategic direction.
  The company minimises the risk of unauthorised access or accidental modifications by restricting access to only those who require it for their roles.

.

Batch Server for Tracking and Storing Code Changes

The company employs a batch server to meticulously track and store all information related to changes made to the source code. This system captures critical details, including:

- **User ID:** The identity of the individual who made the change.
- **Access Logs:** Records of who accessed the code and when.
- **Timestamp:** The exact date and time when the change was made.

This level of granular tracking ensures full accountability and provides a clear audit trail for all activities related to the source code.

5.3. Breach Response and Change Reversion

In the event of a breach or unauthorised change, the company has established protocols to swiftly identify and address the issue. The batch server's detailed logs enable the team to:

- **Highlight Unauthorised Changes:** Quickly pinpoint any alterations that were not approved or were made by unauthorised users.

- **Revert Changes:** Restore the source code to its previous state, ensuring minimal disruption to operations and maintaining code integrity.

6. Resource Management Policy

The company's resource management policy further safeguards against unauthorised access by enforcing strict controls over who can interact with the source code. This policy includes:

6.1. **Role-Based Access Control (RBAC):** Ensuring that access permissions are aligned with job responsibilities.

6.2. **Regular Audits:** Conducting periodic reviews of access logs and permissions to identify and address any anomalies.

6.3. **Employee Training:** Educating staff on the importance of source code security and their role in maintaining it.

The company's approach to source code security is both proactive and comprehensive. By limiting access to authorised personnel, implementing robust tracking mechanisms, and maintaining a clear breach response protocol, the company ensures the safety and integrity of its source code. These measures not only protect the company from potential security threats but also foster a culture of accountability and responsibility among employees.

This policy framework aligns with industry best practices and demonstrates the company's commitment to maintaining the highest standards of security for its critical assets.

7. Capacity Management

The company adopts a proactive approach to capacity management, ensuring that its infrastructure and resources align with both current and future business needs. Senior leadership conducts a thorough review of the existing environment on a quarterly basis. These reviews assess the capacity utilisation across systems, applications, and services, taking into account client requirements and business use cases. Based on the findings, decisions are made to procure or acquire additional capacity management tools or resources. This ensures that the company maintains optimal performance, scalability, and cost-efficiency while meeting the demands of its clients and operations.

8. Management of Technical Vulnerabilities

The company prioritises the identification and mitigation of technical vulnerabilities to maintain a secure and resilient IT environment. Senior leadership may conduct quarterly or annual audits to assess the systems for potential vulnerabilities.

These audits involve:

- Scanning for known vulnerabilities in software, hardware, and configurations.
- Evaluating the effectiveness of existing security measures.
- Implementing remediation plans to address identified risks.

This structured approach ensures that the company stays ahead of potential threats and maintains compliance with industry standards.

8.1. Configuration Management

Configuration management is a critical aspect of the company's IT operations, and the responsibility for this function has been assigned to the DevOps team. To ensure the security and integrity of configurations, the team has implemented the following measures:

8.2. Two-Factor Authentication (2FA):

Adds an extra layer of security by requiring a second form of verification in addition to passwords.

8.3. Strong Password Policies:

Enforces the use of complex passwords that are regularly updated.

8.4. Privileged Access Management (PAM):

Restricts access to sensitive configurations to authorised personnel only, reducing the risk of unauthorised changes.

These measures collectively enhance the security of configuration data and minimise the risk of misconfigurations or breaches.

8.5. Information Deletion

The company has established strict controls over the deletion of information to prevent accidental or malicious data loss:

Restricted Access:

- Only **super admins** and users with specific roles have the authority to delete information. This ensures that deletion actions are limited to trusted personnel.

Data Recovery Policy:

- In the event of accidental deletion, the company can recover data from its **Amazon S3 servers**. This backup mechanism ensures business continuity and minimises the impact of data loss.

By implementing these controls, the company maintains the integrity and availability of its data while mitigating the risks associated with information deletion.
The company's policies and practices in capacity management, malware protection, vulnerability management, configuration management, and information deletion demonstrate a strong commitment to operational excellence and security. These measures are aligned with industry best practices and ensure that the company's IT environment remains robust, scalable, and secure. Regular reviews, employee training, and the use of advanced tools further reinforce the company's ability to adapt to evolving challenges and maintain the trust of its clients and stakeholders.

8.6. Clock Synchronization

The company ensures the accuracy and consistency of time across all information processing platforms through a robust clock synchronization process. The DevOps team is responsible for synchronizing clocks across systems to maintain uniformity in timestamps, which is critical for logging, auditing, and troubleshooting.

8.7. New Systems or Tools

In the event that a new system or tool is introduced, the DevOps engineer is tasked with making the necessary adjustments to ensure seamless clock synchronisation. This includes configuring the new system to align with the existing time standards and verifying its accuracy.
This practice ensures that all systems operate on a unified timeline, reducing discrepancies and enhancing the reliability of time-sensitive operations.

8.8. Use of Privileged Utility Programs

Access to privileged utility programs is strictly controlled to maintain the highest level of security. These programs are only accessible to **senior management**, including the **CEO, CTO, and COO**.

- **Password Management: IP addresses** of devices.
- **Devices attached** to the network.
- **Applications installed** on the system.

To further safeguard these utilities, passwords are periodically changed in accordance with the company's security policies. This reduces the risk of unauthorised access and ensures that only authorised personnel can execute high-level operations.
This stringent access control ensures that privileged utilities are used responsibly and securely, minimising the risk of misuse or compromise.

8.9. Installation of Software on Operational Systems

The company maintains strict oversight over software installations on operational systems to prevent unauthorised or malicious changes.

8.10. Internal Portal and Telemetry Data:

The internal portal collects and stores telemetry data, which includes:

8.11. Daily Reviews by DevOps Security Engineer:

A dedicated DevOps security engineer reviews this data daily to identify any unauthorised installations or changes. Prompt action is taken to address any anomalies, ensuring the integrity and security of operational systems.

This proactive approach helps the company maintain control over its software environment and mitigate potential risks.

8.12. Network Security and Application Security

The company strongly emphasizes securing its network and applications, with the DevOps team playing a central role in implementing and monitoring these security measures.

8.13. Periodic Policy Reviews

Network and application security policies are reviewed periodically to ensure they remain effective and up-to-date with evolving threats.

8.14. Implementation of Security Measures:

The DevOps team is responsible for ensuring that all network security policies and procedures are in place,

including:

- Encryption of data in transit and at rest.
- Use of pins and passwords to secure access to systems and applications.

These measures collectively enhance the company's ability to protect its network and applications from unauthorised access and cyber threats.

8.15. Secure Development Life Cycle (SDLC)

At EarnFlex, we implement a comprehensive and secure Software Development Lifecycle (SDLC) to ensure that all new features and software solutions are secure, reliable, and scalable from inception to delivery.

Our SDLC incorporates security best practices across every phase, including:

- **Secure Design & Architecture**
  We embed security principles such as least privilege, defence-in-depth, and secure design patterns from the earliest stages of product development.
- **Code Reviews & Secure Coding**
  All code is peer-reviewed and follows industry-standard secure coding guidelines to minimise vulnerabilities.
- **Automated & Manual Testing**
  We leverage automated testing (unit, integration, and security scans) alongside manual penetration testing and static code analysis to identify and remediate potential risks.
- **Continuous Integration & Deployment (CI/CD)**
  Our CI/CD pipelines are integrated with security checks and controls to ensure only compliant code is released.
- **Environment Segregation**
  We maintain separate and isolated infrastructure clusters for different clients, ensuring data segregation, minimising cross-tenant risks, and enhancing overall system security.
- **Compliance & Governance:**
  All development practices align with applicable regulatory and compliance frameworks to meet our customers' security and data protection requirements.

Security is embedded into every stage of our development lifecycle to safeguard the integrity and confidentiality of client data while ensuring product excellence.

8.16. Development Process:

The process is divided into several steps, which may follow either a waterfall or agile approach, depending on the project requirements. Key stages include:

8.17. Requirement Analysis:

The development team thoroughly understands the scope and requirements of the project.

8.18. Prototype Development:

A prototype is developed and tested on an **internal server** to validate functionality and security.

8.19. Quality Assurance (QA):

Rigorous testing is conducted to identify and resolve any issues.

8.20. Management Review:

The completed solution is reviewed by management to ensure it meets business and security standards.

8.21. Deployment

Once approved, the code is pushed to the production servers.

8.22. Alignment with Application Security Policy:

Each step of the development process is aligned with the company's application security policy, ensuring that security is integrated into every phase of the SDLC.
This structured approach ensures that new features and software solutions are not only functional but also secure, reducing the risk of vulnerabilities being introduced into the production environment.

The company's policies and practices in clock synchronization, privileged utility program management, software installation oversight, network and application security, and secure development life cycle demonstrate a comprehensive and proactive approach to IT security and operational excellence. By implementing these measures, the company ensures the integrity, security, and reliability of its systems and processes, while maintaining compliance with industry standards and best practices. Regular reviews, strict access controls, and a focus on security at every stage of development further reinforce the company's commitment to safeguarding its assets and maintaining the trust of its clients and stakeholders.

9. Privacy and Protection of Personally Identifiable Information (PII)

Ref: EF-P-08 Technology and Data Protection Policy – Document

We have proactively identified and documented all applicable privacy-related obligations derived from relevant laws, regulations, and contractual agreements.

To ensure robust compliance, EarnFlex Ltd has:

Identification of Requirements

Regularly conducted legal and regulatory assessments to identify privacy-related obligations, including GDPR and other relevant standards.

Documented Policies and Procedures

Clearly documented compliance efforts within our ISMS Policy Statement

Implementation of Controls

Fully established and operationalized procedures and technical controls across our business activities. This includes secure data handling practices, data encryption, restricted access controls, staff training, and clearly defined incident response procedures.

Monitoring and Continuous Improvement

Conducted regular audits and management reviews to validate ongoing compliance, control effectiveness, and identify continuous improvement opportunities.

Conclusion and Statement of Policy

EarnFlex is dedicated to maintaining a secure environment that protects our data, systems, and reputation. Compliance with this ISMS and Cyber Security Policy is mandatory for all employees, contractors, and external partners. Any breach of this Policy is taken very seriously and will result in appropriate disciplinary action, up to and including dismissal or termination of contracts.

By adhering to the principles set forth in this Policy, EarnFlex ensures not only compliance with ISO 27001 and applicable legal requirements but also upholds the highest standards of trust, integrity, and operational excellence. All employees and stakeholders are expected to fully commit to these guidelines, ensuring our collective success and resilience in the face of evolving cyber threats.

For further guidance or to report concerns, please contact a Cofounder. Regular updates and training sessions will reinforce these policies and keep all parties informed of any changes.

Waqas Ahmed
Director
17th March 2025