Foodie: Information Security Assessment Documentation

In accordance with ISO 27001, ISO 27005

# Purpose

The purpose of this document is to outline Foodie's Information Security Assessments in accordance with ISO27001 and SO 27005. Following the scope of ISMS of Foodie, information security policy and objectives, security metrics and monitoring policy of ISMS.

# Information Classification Policy

This policy provides guidelines for the classification, labelling, handling, and de-classification of information assets to protect their confidentiality, integrity, and availability. It applies to all information used in the course of Foodie's activities, whether they are verbally communicated, printed, or stored electronically.

**Classification Levels:** Information assets must be classified into one of the following categories based on sensitivity and business impact:

* Public: Assets in this category are intended for the public and pose minimal risk if accessed without authorization. However, their integrity is crucial to ensure the public receives the correct information.
* Internal: While these assets aren't public, their compromise wouldn't devastate the business. However, they're crucial for smooth internal operations. A change in this data's integrity can lead to internal confusion and inefficiencies.
* Confidential: These assets are vital to the daily operations of Foodie. Unauthorised access or corruption would harm the company's functioning, the integrity and availability of information assets but wouldn't necessarily end the business.
* Top Secret: Assets in this category require the highest level of protection. Any compromise in their confidentiality, integrity, or availability would result in severe consequences, possibly jeopardising the entire business.

**Information Labelling and Handling:**

This is to provide clear guidelines and procedures for the effective labelling and handling of all data and information assets within Foodie. This ensures the protection, confidentiality, integrity, and availability of information, while promoting consistency and efficiency across the organisation.

* No External Share [NES]: This label indicates that the information is of the utmost sensitivity and should not be shared with external parties, even if they have partnerships or vendor agreements with Foodie.
* Eyes Only [EO]: Information bearing this label can only be viewed by specific named individuals.
* Restricted Access [RA]: Data with this label has restricted access within the organisation and is available only to certain departments or roles.
* No Digital Transfer [NDT]: Information bearing this label shouldn't be transferred through digital means and should be communicated only in person.
* Departmental Use Only [DUO]: This label is used for data that is intended only for specific departments within Foodie.
* No Remote Access [NRA]: Information with this label shouldn't be accessed remotely or outside of Foodie's primary premises.
* Need-to-Know [NTK]: Only employees who have a specific need to access this information for their job roles are granted access.
* Encrypted Transfer Only [ETO]: This label indicates that while the data can be transferred within the organisation, it must be encrypted during the transfer.
* Public With Caution [PWC]: Information is public but should be shared cautiously and in the right context to prevent misinterpretations.

**De-classification policy:**

Foodie's De-classification Policy is designed to ensure that our data retains its value while reducing the risk of unintended exposure. As information ages or situations change, the sensitivity and importance of certain data may no longer be applicable. Hence, it becomes necessary to de-classify certain information to optimise resource allocation and streamline access controls.

De-classification can be initiated by the data owner or as a result of the routine reviews. A committee, consisting of the data owner, IT security representative, and a member of the legal team, will review the information. They will evaluate its current relevance, sensitivity, and potential impact if disclosed. A decision will be made about the new classification level, if any. The reason for de-classification, the current and new classification levels, and any other relevant details will be documented. Relevant stakeholders, especially those who interact with or manage the data, will be notified of the changes. If the information is in physical form, new labels will be affixed or old ones removed, as applicable. Digital assets will have their classification metadata updated in the Information Management System.

**Non-compliance:**

Any breaches of this policy could lead to disciplinary measures, and in certain situations, legal implications might arise.

# Information Security Policy

The scope of information security depends on the company's size and it protects the confidential information of clients, its employees and customers and many other stakeholders. This document covers all the information security policies which are related to our ‘Foodie’. It includes all the security roles and responsibilities.

An exhaustive arrangement of proposals and best practices for data security are given by ISO 27002. As indicated by ISO 27002, Foodie ought to contemplate laying out the accompanying significant data security rules, alongside comparing security jobs and obligations:

**Information security rules:**

Security Role: Data security supervisor or boss data security official (CISO).

Responsibilities: Responsibility to create, convey, and deal with the data security strategy are liabilities. Learning consistence of ISO 27002 controls.

**Strategy for Access Control:** ess controls, like client validation, authorisation, and access surveys, are liabilities.

**Data Taking care of and Arrangement Strategy:**

Security Role: Information Proprietor and Information Caretaker are jobs in security.

Responsibilities: It varies among many characterize information arrangement standards, mark information, and ensure grouping based taking care of is done accurately.

**Acceptable Use Policy:**

Security Role: IT supervisor or framework overseer security job.

Responsibilities: Guaranteeing that the acceptable use policy Strategy is followed while utilizing business assets is one of your obligations.

**Information Security Awareness and Training Policy:**

Security Role: Facilitator of preparing and mindfulness for security.

Responsibilities: Create and convey security mindfulness programs, prepare materials, and perform repeating representative preparation as a feature of your obligations.

**Incident Response and Reporting Policy:**

Security Role: Head of the episode reaction group (IRT).

Responsibilities: Driving episode reaction activities, organizing occurrences dealing with, and detailing occasions to the fitting specialists are liabilities.

**Risk Assessment and Management Policy:**

Security Role: Risk proprietor and chance assessor are security jobs.

Responsibilities: Recognizing, assessing, and overseeing security gambles are liabilities. Carry out risk-the-board techniques and watch out for the gamble climate.

**Vendor and Third-Party Security Policy:**

Security Role: Overseeing Merchant Hazard is a security job.

Responsibilities: Assessment and the executives of the security of accomplices and outsider merchants to ensure they stick to security principles.

**Policy for physical security:**

Security Role: Office Chief Security job.

Responsibilities: Executing and overseeing actual safety efforts, access limitations, and hardware and region checking are liabilities.

**Network Security Policy:**

Security Role: Network security manager is a security job.

Responsibilities: Carry out network safety efforts, set up firewalls and interruption identification frameworks, and watch out for network traffic are liabilities.

**Mobile Device and BYOD Policy:**

Security Role: Cell phone the board Director is a security job.

Responsibilities: It is having many characterize the security needs for cell phones, carry out safety efforts, and administer BYOD guidelines.

**Protection Articulation:**

Security Role: Information insurance official (whenever expected by protection regulation) security job.

Responsibilities: Among the obligations are ensuring that information insurance regulations are followed, taking care of solicitations from information subjects, and watching out for information security rehearses.

In conclusion, this report shows the information security policies and their roles and responsibilities in ‘Foodie’. “Foodie” attempts to safeguard its sensitive data and information assets are founded on its information security rules. These policies act as a thorough structure outlining the Foodie's dedication, standards, and practises for protecting important information.

Information Security Objectives & Plans

Making intends to achieve explicit data security objectives is a fundamental stage in carrying out data security the executive’s framework (ISMS) in a Foodie. The Foodie business objectives and the principles of ISO 27001, the ISMS standard, ought to be in accordance with these objectives and procedures. A diagram for creating data security objectives and methodologies for a Foodie is given below:

**Identify Important Information Security Goals:**

Guarantee the classification of significant information by keeping it stowed away from intrusive eyes.

Honesty: To keep information and frameworks precise and extensive.

Ensure frameworks and data are open on a case-by-case basis.

Agree with all authoritative, legal, and lawful commitments connecting with data security.

**Set clear objectives for each goal:**

Confidentiality Objectives: Set up access controls to protect delicate information. Information ought to be scrambled both on the way and very still. Workers ought to get preparing on the worth of information secrecy.

Integrity Objectives: Set information approval looks up as a regular occurrence. Make change the board systems. Lead trustworthiness minds vital frameworks consistently.

Availability Objectives: Execute failover and overt repetitiveness methods. Test the framework's exhibition often. Make an arrangement for business progression and catastrophe recuperation.

Compliance Objectives: Decide appropriate regulations and rules (such GDPR and HIPAA) and ensure you are in consistence. Lead occasional consistency assessments. On the off chance that is essential, lay out a system for revealing episodes to administrative specialists.

**Create Action Plan:**

Make activity designs that indicate the exact techniques, assets, and cut-off times important to achieve every goal and its going with objective.

People or groups ought to be given obligations for each activity plan.

**Risk evaluation and management:**

To find potential security dangers and shortcomings, do an intensive gamble evaluation. Think up risk the board methodologies to lessen or control perceived chances. Allot liability regarding doing gamble with the executives systems.

**Plans for incident response and recovery:**

Make plans for occurrence reaction and recuperation to rapidly manage security episodes. Give insights concerning the episode reaction group's obligations and obligations. Routinely test and amend these plans.

**Auditing and Monitoring:**

Execute progressing checking of the methodology and controls for data security. Direct normal interior reviews to see whether strategies and targets are being followed. To become confirmed for ISO 27001, set up outer reviews.

**Constant Development:**

Make a methodology for the ISMS' continuous improvement. In view of changes in the danger climate and company exercises, much of the time audit and update your data security targets and plans.

**Allocating resources within a budget:**

Spending plan and assets ought to be dispensed as important to assist data security objectives with being met. Remember that data security is a consistent cycle, and objectives and methodologies ought to be inspected and changed occasionally to represent moving circumstances, new dangers, and Foodie extension.We might fabricate a strong starting point for data security inside ‘Foodie’ by sticking to this design and consistently exploring and upgrading your ISMS.

# Security Controls Monitoring & Measurement Policy

Foodie is responsible for coordinating with each control responsibility owner to ensure evaluations are doing well. Security controls and metrics for evaluation are at following:

1. **Access Control Reviews**

* Responsibility: CIO
* Frequency: Monthly
* Monitoring Mechanism: Access Review log
* Parties: All employees, users
* Control Test - Pass: All parties have proper access to all Foodie systems based on the principles of need-to-know and least privilege.

The CIO will Inspect the Access Control to review the access privileges of user accounts every month.

1. **Configuration and Code Change Management**

* Responsibility: CIO and CTO
* Frequency: Ongoing
* Monitoring Mechanism: Tracking of all changes via the help desk ticket system of Foodie
* Assets: Application code files
* Parties: All IT specialists who are authorized to make changes to code.
* Control Test - Pass: All configurations were approved. A ticket exists for each change.

1. **Log Reviews**

* Responsibility: CIO and CTO
* Frequency: Weekly
* Monitoring Mechanism: Secure, access-controlled notes stored in a file repository.
* Asset: Database in Sydney
* Parties: All employees and users
* Control Test - Pass: Log review notes and findings are captured and securely stored. Non-suspicious logs.

1. **Penetration Tests**

* Responsibility: CIO and CTO
* Frequency: Every three months
* Monitoring Mechanism: A third cybersecurity company with a penetration testing team conducts a penetration test on Foodie's application and cloud infrastructure.
* Parties: All employees, third-party company
* Control Test - Pass: Secure frame penetration test results are formally reviewed. Vulnerabilities stemming from penetration tests are tracked and remediated in order of criticality. Vulnerabilities are retested to ensure they no longer exist.

1. **General Risk Assessments**

* Responsibility: CSO, CIO, CTO, CEO
* Frequency: Half year
* Monitoring Mechanism: Foodie risk review
* Parties: All: All employees
* Control Test - Pass: The information system risk review is completed. The risk table is updated with possible risks and risk Scenarios. Existing risks are reviewed. Risks are properly ranting and assigned to different risk owners for risk control and analysis.

# The ISMS internal audit program and the results of audits conducted

For a food delivery company such as "Foodie," the ISMS (Information Security Management System) internal audit program and the results of the audit (as per clause 9.2) relate to a crucial component of ensuring the security and integrity of the company's digital and information assets. It is crucial for the Head of Governance to manage and maintain the company's information security requirements. Here's an explanation:

# ISMS Internal Audit Program

In the context of ISO 27001, Clause 9.2 refers to the requirement for an organization to establish and maintain an internal audit program. ISO 27001 is an international standard for information security management systems. The Head of Governance in Foodie plays a crucial role in ensuring that the company's information security practices meet the standards set by ISO 27001. Here's what this clause entails:

**Internal Audit Program:** Foodie must create a systematic and planned approach to auditing its information security management system. This program is designed to assess and evaluate the effectiveness of the controls, policies, and procedures in place to protect sensitive information and data related to the food delivery service.

**Conducting Audits:** The Head of Governance, along with their team, is responsible for conducting regular internal audits. These audits involve reviewing and examining the organization's information security practices to identify any weaknesses or areas where improvements are needed.

**Audit Scope:** The audit program should define the scope of audits, which means specifying which aspects of the information security management system will be examined during each audit cycle. This could include areas such as data protection, access control, incident response, and more, all of which are critical for safeguarding customer data and maintaining the integrity of Foodie's operations.

**Audit Schedule:** The program should also outline a schedule for when these audits will occur. Regularity is key to ensuring that security measures are consistently effective and up-to-date.

# Results of Audits (Clause 9.2)

Once the internal audits are conducted, the results become invaluable for the Head of Governance and the organization as a whole:

**Identifying Weaknesses:** Audits help in identifying vulnerabilities, gaps, or weaknesses in Foodie's information security management system. This is crucial for mitigating risks and preventing potential security breaches.

**Improvement Opportunities:** The results of the audits provide actionable insights. The Head of Governance can use these insights to make informed decisions about where improvements are needed. This may involve updating policies, enhancing security measures, or providing additional training to employees.

**Compliance Assurance:** By regularly conducting these internal audits, Foodie can ensure that it remains compliant with ISO 27001 standards and other relevant regulations. This is essential for building trust with customers and partners who rely on Foodie to protect their data.

**Continuous Improvement:** The audit program fosters a culture of continuous improvement in information security. It enables Foodie to adapt to evolving threats and challenges in the digital landscape.

In summary, the ISMS internal audit program, as outlined in Clause 9.2 of ISO 27001, is a proactive approach to assessing and enhancing information security within a food delivery service like Foodie. The Head of Governance is pivotal in implementing and managing this program to ensure the security of customer data, regulatory compliance, and ongoing improvement in information security practices.