Customer Name

Information Security Objectives and Issues identified for achieving the Objectives

Information Security Objectives

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Objective | Steps to achieve | KPI | Owner | Expected completed date |
| To understand, develop and implement an ISMS designed to identify, manage, and address potential risks to the company and its customers. | * Engage InfoSec Consultant. * Design and build ISMS (Information Security Management System) | 100% completion of ISO policy documentation + achieve certification |  |  |
| The ISMS should be comprehensive, and the objective is to use best practices to secure the environment and to uphold information privacy rights. | * Clearly document all processes surrounded handling of client data * Identify potential weak points and areas where best practice is currently not implemented as key focal points | 100% documentation completion |  |  |
| The ISMS also should be continuously evolving to address any new threats or vulnerabilities and improve on the existing system. | * Establish at least quarterly review cycle of Customer Name Information Security position. This will be completed via internal audit * Create a culture of feedback, collecting information from the team about new vulnerabilities and threats that emerge as the company grows | 100% of planned audits are carried out on time |  |  |
| The ISMS shall facilitate a secure, trusted environment. | * Provide clear guidelines to employees about information security policies and incident reporting procedures | All employees confirm they are aware of the incident reporting procedures |  |  |
| New and changed portions of the ISMS shall be distributed to management via meetings, communicated to staff, and available for review. | * Establish Management Reporting and Review. * Security awareness training for all staff. | 100% security awareness training completion  100% completion of planned management reviews |  |  |
| All managers will ensure that employees and contract staff understand their responsibilities when protecting information | * Security awareness training for all staff * Ensure that the correct terms and conditions, clauses are in the employment contracts. * Procedures are in place for reporting incidents | All staff trained on incident reporting procedure |  |  |
| Continuously raise awareness amongst all employees and contract staff with regards to information security and associated internal processes, procedures and guidelines. | * Security awareness training for all staff. * Ensure that the correct terms and conditions, clauses are in the employment contracts. * Procedures are in place for reporting incidents | 100% security awareness training completion |  |  |
| The ISMS and related policies and procedures shall be updated at least annually and more frequently if necessary. |  |  |  |  |
| Risk assessments should be performed annually and upon any technology, or business objective changes. | * Creation of an InfoSec Risk Register * Risk Treatment Plan |  |  |  |
| Identified risks will be assigned owners who will endeavor to treat these risks to an acceptable level. |  |  |  |  |
| Identify security breaches and incidents and set target for reduction. | * Continual improvement of InfoSec procedures. | ISMS incident resolution time < 1 week  # ISMS incidents (tracking towards 0) |  |  |
| The ISMS shall provide a governance framework to assist in adopting other compliance standards. | * ISO 9001 * ISO 14000 |  |  |  |
| The ISMS shall enhance capabilities of disaster recovery and business continuity to maintain customer service levels and minimize loss of revenue. |  |  |  |  |
| Acquire the ISO27001 certification through external audit | * Engage InfoSec Consultant. * Plan and complete Internal audits * Plan and complete External Audits leading to Certification |  |  |  |

Identifying issues for achieving objectives of ISMS

|  |  |  |
| --- | --- | --- |
|  | **Positive +** | **Negative -** |
| **Internal** | Strengths   * Motivated and engaged staff * Commitment of Senior Management * Never reported a data breach/leakage to date * Adequate budget for technical tools * Staff have good level of IT knowledge * Reduction of security incidents | Weaknesses   * Security processes are informal and documentation is inconsistent * No internal audits * Low awareness of information security amongst staff resulting in staff being unaware of risks * Complacency amongst staff as they think IT tools will provide adequate protection * Little understanding of requirements of ISO 27001 standard & Data Law * Lack of resources * Inconsistent approach between different sites/departments * If international - language/communication issues * IT outsourced but outsourced company is no proactive |
| **External** | Opportunities   * ISO 27001 certificate will allow us to enter new customer marketplaces * Improved compliance with legal and contractual * requirements * Improved relationships with clients | Threats   * New Cyber emerging threats * Little understanding of relevant regulatory requirements - Data protection and privacy legislation such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) and the Data Protection Act 2018 (DPA 2018) * Political influences e.g. Brexit * Not being able to meet privacy needs/requirements from customers or potential customers * Note being able to get required privacy requirements from our vendors/suppliers * Keeping up with changing legislation and privacy landscape globally |

Complete this template using the Clause 4 self-help guidance document after discussing and exploring the current and potential issues for achieving the ISMS objectives.

Store this document within the Clause 4 folder for future reference. It should be reviewed annually and if new issues are identified.

|  |
| --- |
|  |

Provided by

Logo

Description automatically generated