Quality Management Document:

Information Security Summary

Summary:

High Level Information Security Summary to provide an outline and justification for risk-based information security management.

Document Control

Document Title:	Information Security Summary
Version:	V1.0
Release Date:	28th April 2020
Issue No:	1.0
Authored By:	Daryl Greensill
Approved By:	Information Security Group
Doc Class	Public

t: 01226 212056
f: 01226 249625
w: www.targetis.co.uk

Target Information Systems Limited
Innovation Way
Barnsley
S75 1JL

VAT No: 993 2148 96
D&B DUNS: 216672692

Registered in England & Wales, Company No: 07209070

Contents

1 Purpose

Information that is collected, analysed, stored and communicated is at risk of theft, misuse, loss and corruption.

Information may be put at risk due to poor education, training and breach of security controls.

Information security incidents can give rise to embarrassment, financial loss, non-compliance with standards and legislation.

This high-level policy sits alongside other Target Information Systems policies to describe and control the entire information security risk.

2 Objectives

Target is committed to operating an Information Security Policy that:

- Risks are identified, managed and treated according to the agreed risk tolerance.
- Authorised users can securely access and share information to perform their roles.
- Physical, procedural and technical controls to balance user experience and security.
- Contractual and legal obligations are met and exceeded.
- Individuals accessing our information are aware of their responsibilities.
- Incidents affecting our information assets are resolved and learnt from.

3 Scope

The Information Security Policy and its supporting controls, processes and procedures apply to all information used, in all formats.

This Information Security Policy and its supporting controls, processes and procedures apply to all individuals who have access to Target Information Systems information and technologies.

4 Compliance

Compliance with controls in this policy will be monitored by the Information Security Group and reported to the Senior Management Team where appropriate.

5 Policy

It is the policy of Target Information Systems that information is protected from a loss of:

- Confidentiality – information will be accessible only by authorised individuals
- Integrity – the accuracy and completeness of information is maintained
- Availability – information will be accessible to authorised individuals when required

5.1 Information Security Policies

A set of lower level controls, processes and procedures for information security will be defined in support of the high-level policy and its objectives. These supporting controls will be approved by the Information Security Group, published and communicate to all relevant individuals.

5.2 Access Control

Access to all information will be controlled and driven by business requirements. Access will be granted based on an individual's role and classification of information, only to a level which will allow them to carry out their duties.

- Access must be granted to individually authorised users with no shared credentials where possible.
- Access must be based on need to know and a principle of least privilege.
- Requests for user accounts and raised privileges must be documented and approved.
- Access must be reviewed/removed as part of the starters/leavers/movers process.

5.3 Backup Policy

To maintain integrity and availability of information it is important that all information is securely backed up in case of accidental or malicious damage. The backup process should ensure that information is securely stored while minimising the impact to users.

Data owners are responsible for determining what backup and resilience arrangements are required to protect the information for which they are responsible.

Backup of data held in database systems shall have data backup routines which ensure database integrity is retained. By default, databases should be backed up daily and daily working copies stored for a rolling 7 days. Full database backups should be stored monthly and retained in line with the data retention policy.

5.4 Business Continuity

The Business Continuity Plan aims to assess risks and plan for crisis mitigation across all areas of the business. The policy includes sections to cover Risk Management, Crisis Management and

Disaster Recovery. The plan also includes several previously identified scenarios and the plans relevant to mitigate each of them.

For more information see the Business Continuity Plan.

5.5 Change Management

Change Management provides a process to apply changes, upgrades or modifications to Targets operation procedures or infrastructure. The Change Control process and Change Control Register are defined to document planned changes, identify risks and put in place controls to minimise risk.

5.6 Encryption

Where appropriate all sensitive information is encrypted to protect confidentiality, authenticity and integrity of information.

5.7 Information Handling

All information that is processed, stored or distributed by Target employees should be handled appropriately. All data shared with or by Target shall be done via a secure method. All portable devices must be encrypted at rest, and all data transferred online must be via a secure encrypted communication channel.

Data will only be used on behalf of a client to enable the delivery of a provided service. Customer data will be stored on a secure storage location, with appropriate access controls and backup procedures.

To minimise risk, all data should only be stored for as long as needed. Once the purpose for handling the data is no longer relevant it shall be deleted.

5.8 Information Risk Assessment

All individuals have a duty to assess information risks by looking at the asset, the vulnerability (ease which an asset can be exploited) and the threat (the likelihood of this happening). All risks should be recorded in the Risk Treatment Plan.

5.9 IT Usage Policy

Users have a responsibility to promote IT security and must safeguard the electronic information and systems within their care and use. The IT Usage Policy defines responsibilities, restrictions and controls to ensure that all systems retain security and integrity.

5.10 Password Policy

Passwords are the primary method of user authentication. The password policy defines best practice to how users should create and use passwords to minimise risk of account credentials being compromised.

All passwords for business related systems should be unique and not reused in other systems.

Where a system cannot enforce a strong password then users should be aware of what represents a strong password and ensure that they self-select a password that meets this policy.

In systems developed by Target, all passwords should be encrypted using an appropriate method such as SHA 512 using a random salt and random iterations on a per password basis.

5.11 Secure Development and Deployment Policy

The Secure Development and Deployment Policy identifies best practices that should be followed in every element of software development.

All user inputs are validated, sanitised and encoded before display to preview XSS attacks. Every action that changes data uses a Cross-Site Request Forgery (CSRF) token to prevent request forgery.

Production systems are only deployed to server providers and data centres which are IS027001, SOC Type I/II and PCI-DSS accredited. Live and test environments are deployed onto different servers using a common configuration.

A perimeter firewall is configured to only allow external access to a Web/proxy server and SSH via an SSH Tunnel. The Web/proxy server runs a Web Application Firewall to filter common attack vectors. Servers are configured with appropriate security software including Log File Analysis, automatic firewall configuration/blocking and Intrusion Detection Systems.

5.12 Supplier Security

Security should be considered when establishing relationships with suppliers to ensure security is maintained through the entire supply chain. The Supplier Security policy defines a set of controls for selecting and working with suppliers. This includes identifying and managing risk, managing the contracts and ensuring that Information Security is considered across the entire supply chain.

5.13 Starters, Movers and Leavers Policy

When employees join, move roles or leave the organisation there is a high possibility that requirements for access to information changes. The Starters, Movers and Leavers Policies put in place a set of controls for managing the change, ensuring that the principle of least privilege is maintained across the entire organisation.