Information Security Policy

Digital networks connect Halton customers, partners and employees and equipment across the group countries through information technology, automated control systems, the Internet and social media. Operations depend on these networks. Therefore a risk management practise is being established to identify, manage and mitigate information security threats and risks.

With this policy management wants to express the most important guidelines and focuses for information security activities and its commitment to information security in its operations.

Halton manages and produces information that is private, confidential or sensitive in nature, together with information that is regarded as being readily available for general sharing. The Halton recognises that it is imperative that all information is protected from compromise of confidentiality, integrity and availability. All within the scope of the policy must therefore ensure that:

- Selected key processes, technology, services and facilities are protected through information security controls (CIS Controls).
- Information security incidents are identified, contained, remediated, investigated and reported to the Chief Information Security Officer (CISO).
- Where appropriate, a risk assessment is carried out on processes, technology, services and facilities.
- Back-up and disaster recovery plans, processes and technology, are in place to mitigate risk of loss or destruction of information and/or services and to ensure that processes are in place to maintain availability of data and services.

In addition, all individuals within scope of the policy:

- Have possbility to participate the information security awareness training.
- Ensure that reasonable effort is made to protect the Halton’s information and technology from accidental or unauthorised disclosure, modification or destruction.

Scope

- Everyone within the Halton who accesses Halton information assets or technology. This includes Halton customers, users, consults and external parties
- Technologies or services used to access or process Halton information assets.
- Information assets stored and/or processed in relation to any Halton function, including by, for, or with, external parties.
- Information that is transferred from and/or to the Halton for a functional purpose.

Objectives

- Protect the Halton’s information and technology against compromise of confidentiality, integrity and availability by identifying, managing and mitigating information security threats and risks.
- Support the Halton’s strategic vision through an approach which effectively balances usability

and security.
- Facilitate a 'security aware' culture across Halton units world-wide and promote that information security is everyone's responsibility.
- Define security controls that are effective, sustainable and measurable.
- Identify, contain, remediate and investigate information security incidents to maintain and assist in improving the Halton's information security posture.
- Ensure the Halton is compliant with its information security obligations
- Provide assurance to other parties that we have a robust control environment in place to protect their data through an effective information security management system.

Responsibilities

Aki Saxén, Chief Information Security Officer (CISO) manages and develops information security policy on behalf of the Halton group.

Halton Enterprise Architecture Council reviews and approves the information security policy and its supplemental guidelines. List of members can be found from Halton intranet.

Management has responsibility for information security within their units. They must actively support the adoption and implementation of the information security requirements, policy and framework as well as ensuring compliance within their areas of responsibility. They are also responsible for the unit's internal communication on information security.

Users are responsible for protecting the Halton's information and technology systems and for complying with regulations and policies. Where an individual user suspects personal data may have been compromised or if a user suspects or discovers any material breach of the requirements detailed within this policy, they must report this to the Chief Information Security Officer.

Compliance

This Policy is reviewed on a periodic basis to ensure they remain accurate, relevant and fit for purpose.

Any violation of this policy or applicable local laws may be subject to investigation and/or disciplinary actions or other remedies/ sanctions under the applicable law, employment or service contracts. Questions concerning any aspect of this policy should be directed to the Halton Human Resources department.

Version control and approval

Version	Editor	Date	Version / Revision Comments
0.1	Aki Saxén	03.08.2018	Initial Draft
0.2	Aki Saxén	10.08.2018	Draft, Minor changes
0.3	Aki Saxén	16.08.2018	Draft, Minor changes
0.4	Aki Saxén	18.09.2018	Draft, Changes to introduction and Structure
0.5	Aki Saxén	15.11.2018	Draft, Changes to introduction text
1.0	Aki Saxén	27.12.2018	Final, Approved version

Reviewer/approver list

Name	Role	Comments	Review/Approval
Aki Saxén	CISO		Creator, Reviewer
Legal	-		Reviewer
Human Resources	-	Group HR Director	Reviewer
Regional IT Responsibles	-	Consulted with US & European IT personnel	Reviewer
EA Council	-	Consists members from all SBA´s and Group	Reviewer, Approver

Policy