Guide to Security in the Legal Standards Framework v2.0

I. POLICY AND ORGANIZATION

Current Information Security Policy and Organization of Information Security

1.1	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	ISO 27002:2013 §5.1.1
1.2	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	ISO 27002:2013 §5.1.2
1.3	All information security responsibilities shall be defined and allocated	ISO 27002:2013 §6.1.1

Risk Analysis

1.4	Sonic Foundry performs at least every 3 years a risk assessment to determine and mitigate threats and vulnerabilities, and the consequences that result from these effects. Based on the risk assessment, adequate security controls are defined and implemented.	ISO 27001:2013 §8.2 ISO 27005:2011 §12.1
1.5	Sonic Foundry describes how identified risks will be treated and substantiate why residual risks are accepted.	ISO 27001:2013 §8.3 ISO 27005:2011 §9 en §10

Awareness and Training

1.6	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	ISO 27002:2013 §7.2.2

Incident Management and Data Breaches

1.7	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents. The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	ISO 27002:2013 §16.1.1 ISO 27035:2011 NIST SP800-61r2
1.8	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	ISO 27002:2013 §16.1.1 ISO 27035:2011 NIST SP800-61r2
1.9	Information security incidents shall be responded to in accordance with the documented procedures.	ISO 27002:2013 §16.1.2 ISO 27035:2011 NIST SP800-61r2
1.10	The organization has defined an incident classification frame to classify incidents based on urgency and impact.	ISO 27002:2013 §16.1.4 ISO 27035:2011 NIST SP800-61r2
1.11	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	The Personal Data Protection Act of the Netherlands Article 14 Sections 2.1-2.4

Change Management

1.12	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	ISO 27002:2013 §12.1.4, §14.2.6, §14.2.9 PCI DSS v3.2 §6.4.5.3
1.13	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	PCI DSS v3.2 §6.4.5, §6.4.5.1, §6.4.5.2
1.14	Changes are made within the agreed service time window and large impact changes are consulted with the client before the change is implemented.	PCI DSS v3.2 §6.4.5, §6.4.5.1, §6.4.5.2
1.15	Sonic Foundry documents the new situation after a change in the CMDB (configuration database) has been made.	ISO 27002:2013 §12.4.1

Continuity Management

1.16	Sonic Foundry has demonstrable preventive and corrective measures in place for the realization of requirements concerning availability.	ISO 27002:2013 §12.4.1
1.17	Sonic Foundry knows the single point of failures in their infrastructure and has controls in place to solve interruptions within agreed time frame.	ISO 27002:2013 §17.1 en §17.2
1.18	Sonic Foundry continuously monitors the availability and capacity of applications.	ISO 27002:2013 §12.1.2 en §12.1.3
1.19	Sonic Foundry creates back-ups according to availability requirements.	ISO 27002:2013 §12.3
1.20	Sonic Foundry saves backup copies securely off-site. The distance between the primary storage location and the backup location should be at least 5 kilometers.	ISO 27002:2013 §12.3

Privacy

1.22	Sonic Foundry has a non-disclosure agreement used by employees and third parties.	
1.23	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. In case of Risk level 2 a VOG should be handed by the candidate.	

II. ACCESS SECURITY

Physical Access Security and Equipment Security

2.1	IT assets shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access and no damage or interruptions can occur due to this. The measures that are taken cover the identified risks.	ISO 27002:2013 §11.1 en §11.2

Logical Access Security

2.2	When designing user access management the following rules should be included: • users and administrators use unique login ID's combined with a password, • shared login ID's and passwords are not allowed • users shall only be provided with access to the network and network services that they have been specifically authorized to use	ISO 27002:2013 §9.1 en §9.2.4

2.3	Sonic Foundry has a policy for the use of mobile devices and includes: • the requirement that the mobile device has a key lock or a something that is comparable, e.g. access via a password, • private and business use are separated and company data may only be stored on an encrypted device.	ISO 27002:2013 §6.2.1 en §11.2.8
2.4	A formal user registration and de-registration process shall be implemented to enable assignment of access rights. The access rights process should at least include: • a registration of users and the access rights they received, • ensure authorized user access and to prevent unauthorized access to systems and services they do not need to have access to • access rights shall be removed upon termination of employment, contract or agreement, or adjusted upon change.	ISO 27002:2013 §9.2.1, §9.2.2, §9.2.3, §9.4.1 en §9.2.6
2.5	Users and administrators are being informed about the access rights policy and have to sign a statements that they will not share personal secret authentication-information and when there is a case of infringement they will take actions to limit the effects.	ISO 27002:2013 §9.3.1
2.6	Sonic Foundry checks monthly if the provided access rights are correct.	ISO 27002:2013 §9.2.5
2.7	Based on the access rights policy Sonic Foundry has a secure login procedure for systems and applications. The login procedure will have a strong password. Based on a risk analysis a stronger password (multi-factor authentication) could be needed for specific applications.	ISO 27002:2013 §9.4.2, §9.4.3

III. MANAGEMENT OF TECHNICAL VULNERABILITIES AND ANTI-MALWARE

Vulnerability Management

3.1	Sonic Foundry has a process that prevents exploitation of technical vulnerabilities. The process includes: • regularly update the systems and software (patching), • Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion (intelligence), • network and systems shall be controlled against vulnerabilities(vulnerability assessment), • testing of web applications, on a regular basis, against vulnerabilities (Web application scanning), • the use of anti-virus software that is updated daily, • restricting the installation of (unauthorized) software.	ISO 27002:2013 §12.2, §12.6.1, §12.6.2 en §14.2 ISO 27033-1:2015 §8.3

Intrusion Detection

3.2	Sonic Foundry inspects the transport of data from external or untrusted networks in real time.	ISO 27033-1:2015 §8.5 en §8.6

IV. CONFIDENTIALITY AND INTEGRITY OF DATA, PRIVACY

Protection of Personal Data

4.1	Sonic Foundry has a privacy policy that is not older than 3 years.	ISO 27002:2013 §18.1
4.2	Sonic Foundry has appointed a privacy officer.	The Personal Data Protection Act of the Netherlands Article 18.1

Encryption

4.3	Stored media containing confident information shall be encrypted for the following: • removable media (e.g. external saved back-up tapes, DVD's, memory cards and USB-sticks); • the memory of mobile devices (e.g the internal and external memory of laptops, smartphones and tablets).	ISO 27002:2013 §10.1, §13.2, §14.1.2
4.4	End-to-end encryption is always necessary when data is classified as sensitive or critical and has to be transported (e.g. making a back-up). Sonic Foundry encrypts confident data that have to be transported in the following situations. • administrator activities on the private network (using encryption facilities within the administration tools or protocols used); • wireless data communication; • passwords that need to be stored or sent.	
4.5	Sonic Foundry uses current available techniques for encrypting connections and hashing algorithms	ENISA Algorithms- key-size-and-para- meters-report-2014
4.6	Sonic Foundry uses hardware solutions(e.g. smartcars and Hardware Security Module products) that are certificied according to security standards.	
4.7	Media shall be disposed of securely (using secure erase) when no longer required	ISO 27002:2013 §11.2.7 NIST §14.5.7

V. CONTROL AND LOGGING

Control and Logging

5.1	Event logs recording user activities at the level of a person and registers the amount of successful and failed login attempts.	ISO 27002:2013 §12.4.1
5.2	Logging facilities and log information shall be protected against tampering and unauthorized access.	ISO 27002:2013 §12.4.2
5.3	System administrator and system operator activities shall be logged and the logs shall be protected and regularly reviewed.	ISO 27002:2013 §12.4.3
5.4	The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source.	ISO 27002:2013 §12.4.4
5.5	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed. These logs will be shared with the client. The logs include: • the amount of successful and failed login attempts • date and time of the failed login attempts; • the requested and approved access to files/information outside business hours; • activities by administrators; • significant user activities (e.g. mutations to authorizations, configuration settings, etc.); • detected malware (worms/viruses/spyware e.d.)	
5.6	Sonic Foundry will save all log files for at least 3 months and at most 12 months. During this time the client will have access to this information. When the law has defined other terms, these should be followed.	The Personal Data Protection Act of the Netherlands Article 10.1 and 10.2