WUR Information Security Policy

DATE
31 Maart 2021

AUTHORS
Luc Boelhouwer
Remon Klein Tank

VERSION
1.4

STATUS
Final

CONFIDENTIALLITY
Public

Maintenance and approval

This document has been approved on 08 / feb / 2021 by the Executive Board and will be communicated to all interested parties within the organisation and when necessary to relevant parties outside the organisation.

Wageningen University & Research shall ensure that this policy and related documentation are reviewed regularly and if necessary are updated with organizational adjustments or technological changes.

1. Introduction

1.1 Purpose

The Information Security Policy (hereafter the "Policy") lays out Wageningen University & Research's (WUR) approach to information security management. The Policy is in place to support the mission of WUR and to facilitate the protection of WUR's information and technology services against any compromise of its confidentiality, integrity and availability. Whilst doing this, it recognises that the ability to develop and deliver educational services, perform research and create value must be maintained, therefore WUR strives to achieve the following:

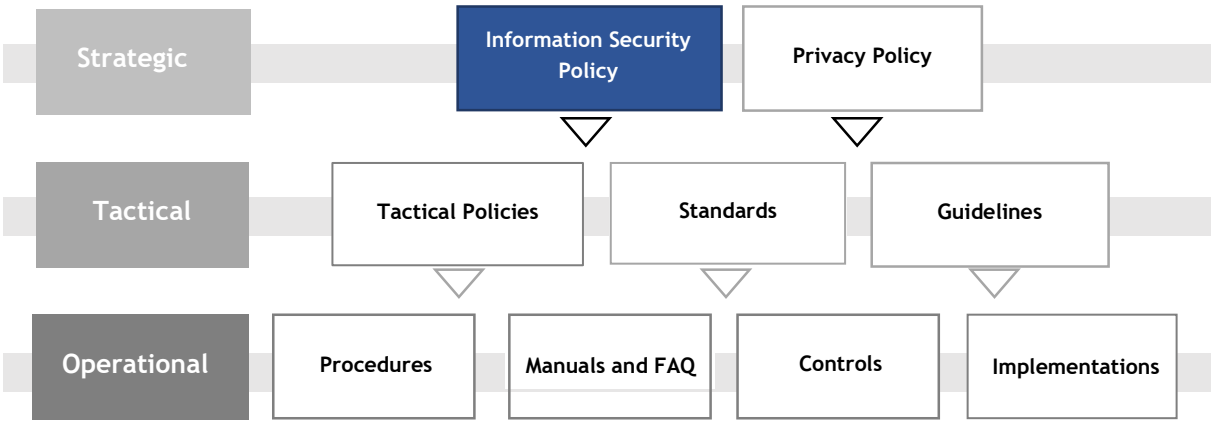
- Ensure the availability of information when it is needed for education, research and business operations.
- Ensure the information is correct, complete and actual over its entire lifecycle (integrity). Additional attributes like authenticity, reliability and non-repudiation can be considered a subset of integrity.
- Ensure that information is accessible only to those who are entitled to this information based on their function/role (confidentiality).
- Prevent security and privacy incidents and lower the impact of incidents that do occur.
- Define security controls that are effective, sustainable and measurable.
- Contribute in the compliance of contractual, legal or regulatory obligations.
- Support the execution of WUR's mission and primary processes of Education, Research and Value Creation through an approach that effectively balances usability and security.
- Facilitate a 'security aware' culture across the WUR and promote the idea that information security is everyone's responsibility.
- Create trust among stakeholders that WUR has a robust control environment in place to protect their data using an effective Information Security framework.

1.2 Information security and privacy

Information Security and Privacy are distinct but interrelated terms, and since Privacy cannot be achieved without Information Security, we take a coordinated approach at tactical and operational level. The starting point for information security is the determination of information security risks. From there, WUR takes preventive, detective, reactive and corrective measures to guarantee the confidentiality, integrity and availability of WUR's data and information services.
Information security has a strong connection with privacy (protection), which encompasses all manners of protecting *personal data*. Privacy is described in WUR's Privacy Policy and is a responsibility of the Privacy Officer.

1.3 Information Security framework

This Information Security Policy describes WUR's approach to information security to support it's mission "To explore the potential of nature to improve the quality of life" and protect our primary education, research and value creation processes. This document describes high-level objectives, policy statements and governance, and is designed to be in line with Wageningen University & Research mission. This policy is subsequently translated into tactical policies, standards and guidelines, which specify specific security measures and will be updated more frequently and tailored to the needs of the organization.



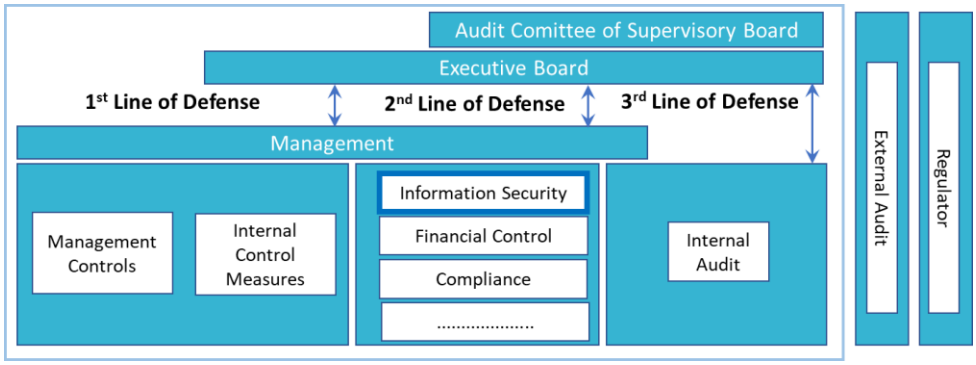
1.4 Scope

The scope of this policy includes:

- All employees, including permanent and temporary employment, students, contractors, consultants, visitors, suppliers, alumni, and any third party engaged to support WUR activity and who therefore has authorised access to any of WUR's information assets.
- All primary and supportive (business) processes and all underlying information systems and data;
- Information assets owned by WUR or processed in relation to any WUR function, including by, for, or with, external parties.
- Third party, public, civic or other information that WUR is storing, curating or using on behalf of another party.
- All areas, buildings, objects and equipment of WUR (physical security) in relation to information and data;

2. Governance & Responsibilities

For the internal organisation of information security, WUR uses the so-called 'Three Lines of Defense model', which implies that responsibilities and risk ownership are assigned to the business operations and involve the following activities:



i. The first line of defense (functions that own and manage risks).
This consists of managers and staff who are responsible for identifying and managing risk as part of their accountability for achieving objectives. Collectively, they should have the necessary knowledge, skills, information, and authority to operate the relevant policies and procedures of risk control. This requires an understanding of their business, its objectives, the environment in which it operates, and the risks it faces.

ii. The second line of defense (functions that oversee or specialise in compliance or risk).
This provides the policies, frameworks, tools, techniques and support to enable risk and compliance to be managed in the first line; monitors in order to judge how effectively they are doing it; and provides help and advice in order to ensure a consistency of definitions as well as the measurement of risk.

iii. The third line of defense (functions that provide independent assurance).
This is provided by internal audit. Sitting outside the risk management processes of the first two lines of defense, its main roles are to ensure that the first two lines are operating effectively and to advise how they could be improved. It can also give assurance to regulators and external auditors that the appropriate controls and processes are in place and are operating effectively.

In the above model WUR recognizes the following responsibilities for information security:

2.1 First and foremost, it is everyone's responsibility to handle information (systems) properly, securely and in accordance with applicable WUR guidelines.

2.2 This Policy is owned, managed and developed by the Chief Information Security Officer (CISO) on behalf of the WUR Executive Board.

2.3 This Policy is reviewed and approved by the Executive Board through the governance route of Architecture Board (AB).

2.4 The (Sr.) Information Security Officer (ISO) is responsible for maintaining an overview of the threat landscape that, combined with the business data classification, is the input for a risk-based approach to cybersecurity. The ISO advises on the implementation of controls that reduce risks to a level that is acceptable for WUR.

2.5 The domain IT executes the following centralized information security process: Incident Management and Emergency Response, Back-up and Recovery, Data Breach registrations and IT Change Management.

2.6 The Science Group Operations Director or CS+ Director is accountable for ensuring that adequate and effective information security controls are in place within their area of responsibility. They are also accountable for compliance in any subsidiary unit, for example, associated institutes, research groups and multi-disciplinary organisations within their management.

2.7 The Data Controller is appointed to be responsible for a dataset within WUR (which is not necessarily equal to the legal owner) and determines the purpose and means of processing that data in line with this Policy. If the data includes any personal data, they also need to adhere to the Privacy Policy. The Data Controller responsibilities are further defined in the Standard under 'The Data Controller role'.

In addition, the following have information security responsibilities:

2.8 Senior Management and associated Governance committees have executive responsibility for information security within WUR. They must actively support the adoption and implementation of the information security Policy as well as ensure compliance within their areas of responsibility. Senior management for this purpose is defined as Executive Board (RvB), Board of Directors (Concernraad) and Deans (Dean of Education and Dean of Research).

3. Policy Statement

This Policy advocates a holistic approach to information security and risk, which entails first identifying and assessing information security threats, and subsequently developing and implementing a combination of people, processes and technology controls to mitigate those risks according to WUR's desired objectives.
The Information Security Policy is based on international ISO27001 standards with agreed additions and adaptations for the Higher Education sector in the Netherlands (through SURF and VSNU). This implies that information security is a managed process based on risk.
WUR has defined five security principles to help determine which controls are needed to achieve the objectives in this scope. The practical details and effects of these principles are described in the Tactical Policies, Standards and Guidelines.

1. Risk based

Information security controls are based on WUR-specific risk assessments and analyses, and are carried out in line with the laws and regulations. Risks are evaluated, analysed and owned by the person responsible for the data in question (data controller). By selecting the appropriate controls, WUR achieves effectiveness and efficiency regarding the value (classification) of information (systems) and the benefits of the intended improvement.

2. Everyone

All employees, students, guests and third parties should be aware of their responsibilities concerning a proper and secure handling of information (systems). Since everyone's participation is vital to the success of this policy, WUR actively promotes information security measures.

3. Always

Considering how the information management environment is continuously changing and how cyber threats are evolving, WUR's information security is maintained through a constant process of risk assessment, by updating controls and enhancing awareness in order to ensure ongoing state-of-the-art security levels.

4. By design

Appropriate information security requirements constitute an integral part of every project or change related to information (systems), processes and IT-facilities – from start to finish. Access controls are designed to ensure that users only have access to information necessary to the fulfilment of their respective tasks and responsibilities (provided on a need-to-know basis).

5. By default

Implemented configurations will have available security options enabled. Access is restricted by default to protect the user from accidental and unwanted sharing of information. Deviation from default secure configuration is a risk and can only be accepted as a risk by the one responsible for the data.

Data classification

Data classification is a crucial part of the risk-based approach described in the first principle. WUR manages and produces information. When this information is lost, altered, or publicly disclosed it can have an impact on WUR. WUR therefore categorizes all data depending on the level of potential impact (damage) if the data loses its integrity, confidentiality or availability. In these cases, the impact can concern the institution's image, primary processes, personal data, or finances. The four impact categories are: 1) 'negligible' 2) 'some' 3) 'serious' and 4) 'disruptive'.
A lot of data that WUR processes are considered open information at some point and are thus available to the public. Data classification does not limit with whom data can be shared, but rather regulates the security baseline for the information systems that are used. Open information can harm WUR if its integrity or availability is not protected. WUR thus recognizes that it is imperative that all information be adequately protected from any compromise of confidentiality, integrity or availability.
The risk appetite, the classification process and the required controls are described in the 'data classification standard'.

All stakeholders within the scope of the Policy must make sure that:

3.1 Information assets are identified, classified and protected in accordance with the associated documentation and standards. Any security controls implemented must be proportionate to the defined classification. Key information assets are governed by an appointed Data Controller in accordance with the associated documentation.

3.2 All processes, technology, services and facilities are protected through information security controls as detailed in the associated Standards.

3.3 Information security incidents are identified, contained, remediated, investigated and reported in accordance with the Incident Management Standard.

3.4 Where a third-party provider is employed for any services involving contact with WUR information, an information security risk assessment is carried out to ensure that they comply with WUR's Information Security Policy and Standards.

3.5 Where appropriate, an information security risk assessment is carried out on all processes, technology, services and facilities in accordance with the associated standard in order to bring risks within the acceptable range.

3.6 Back-up and disaster recovery plans, processes and technology are in place in accordance with the Business Continuity Standard 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.

3.7 Where off-site or remote working takes place, appropriate security controls are implemented in accordance with the associated standards.

4. Compliance

This Policy can be met by adopting and complying with the associated Standards, however, it is designed to be flexible: a range of methods is allowed to facilitate meeting this Policy. This enables local autonomy, insofar as local procedural methods and/or controls may to be implemented in order to fulfil the outcomes and objectives of this Policy. At the same time, it allows those who require further advice from the Information Security Office to meet this Policy through the methods detailed in the Procedures. Regardless of the approach, all stakeholders within scope of the Policy are required to meet this Policy and the Standards using appropriate methods.

It is important to note that the standards, as outlined in the associated documentation, must be considered the minimum requirements (or the 'baseline') for information security. Where additional information security controls are required for research, legal, regulatory or governance purposes, the controls must be enhanced accordingly. The Information Security Office can provide advice on how to comply with additional security requirements where required.

4.1 This Policy and the Framework are reviewed on a periodic basis by the Information Security Office to ensure they remain accurate, relevant and fit for purpose.

4.2 The Information Security Office may carry out periodic compliance and assurance activities (e.g. assessment of security controls) to ensure that they are aligned with this Policy.

4.3 Failure to meet requirements detailed within this Policy may result in the user being subject to formal disciplinary action according to the relevant disciplinary code or procedures. Additionally, where it is suspected that an offence has occurred under Dutch law, it may also be reported to the compliance officer or other appropriate authority.

4.4 There will be a Coordinated Vulnerability Disclosure statement which will encourage the reporting of vulnerabilities to WUR and detail conditions for not taking disciplinary or other legal steps if the reporting is carried out accordingly.