Procedure Security Check

Purpose

When using a tool, application or system, data of the university are stored and/or processed. This can be all kinds of data. For example, data that relate to the business of the university, such as financial data, but also data about students and employees (personal data). It is important that these data are safely stored. As a university, we set requirements for this, also known as security requirements. These security requirements can be divided into technical and organizational requirements.

- Technical security is about ICT security. This includes the security of applications, the network, access controls, backup, and encryption of data. You can find the requirements in the Security Technical IT Checklist (STITCH).
- Organizational security is about the way in which data is handled. For example, who can view and process which data, what is the password policy and are employees trained in the field of security. You can find the requirements in the SURF's Legal Standards Framework for (Cloud) Services.

The technical check is done by the IT-Security team. The organizational check is conducted by the CISO-Office team.

Procedure	
When? - When purchasing or tendering* a new tool, application, system or service. - When modifying an existing tool, application, system or service. *In the case of a tender, the technical and organizational security requirements are included as part of the tender documentation by the Procurement and Contract Management department.	

Stage	Who	What	How	Processing time
1	Information Manager division or school	Send a request for a security check by e-mail.	Mail to security-testing@tilburguniversity.edu the following: • Indicate that you intend to purchase a tool, application, system, or service • Provide the necessary information in advance • Name of application and supplier • Name of system owner • What is the purpose of the application? • What data will it process? • BIV application classification	
2	IT-Security team CISO-Office team	You will receive a confirmation that your application has been registered, including a Topdesk number.	By e-mail.	+/- 1 week
3.1	Informatie Manager division or school	Request information from the supplier in advance. The sooner information is available, the quicker the security check can be carried out.	Contact the supplier: • Ask for certifications (such as ISO 27001 with accompanying Statement of Applicability), periodic checks/audits and process descriptions. • Ask for a pen test report. To check the technical security, we use the Security	+/- 2 weeks (depending on the speed of response from the supplier)

			Technical IT Checklist (STITCH). The easiest way for a supplier to prove STITCH compliance is through a pen test report from an independent tester. If necessary, we are prepared to sign a non-disclosure agreement (NDA) because these reports are often confidential. • We use the SURF Legal Standards Framework to check the organizational security.	
3.2	Information Manager division or school		Send the information you received from the supplier to security-testing@tilburguniversity.edu.	
4	IT-Security team CISO-Office team	The IT-Security team and the CISO-Office assess the results and determine whether they comply with the security requirements and/or whether or not they accept deviations from them.	Based on the information sent at 3.2.	+/- 2 weeks
5	IT-Security team CISO-Office team	You will be informed of the outcome of the check in a motivated manner. The result will be provided with a colour code*.	By e-mail, in Topdesk ticket.	

*Explanation of colour codes:

- GREEN: we have seen/received convincing evidence that the application or service is sufficiently secure according to our security requirements. This means that the application can be used secure.
- ORANGE: we do not have the complete information available to come to a "GREEN" result, but also found no matters which give some reason to give a "RED" result. The use of the application therefore involves a security risk. The risks are described by us in a Risk Information Form (RIF), which will be shared with the system owner and responsible director. The choice of whether to accept the risk is up to the system owner and director.
- RED: we have actual reason to believe that the application or service is so insecure that our urgent advice is to NOT use the application or service. The risks are described by us in a Risk Acceptance Form (RAF), which will be shared with the system owner and the responsible director. The choice of whether to accept the risk is up to the system owner and the director. The signed form will also be shared with the Executive Board.