

Schedule 3 - Service Provider Security Measures

1. Information Security Requirements

- 1.1** The Service Provider shall implement the requirements specified in this document. The implementation of and compliance with these requirements shall be reviewed by Service Provider on a regular basis. Alternative protection measures are only permissible if approved in advance by SEFE.
- 1.2** Employees of the Service Provider who have access to company information and systems must be aware of the requirements set out in this document.
- 1.3** The Service Provider must ensure that subcontractors also comply with all SEFE's information security requirements resulting from this document in the context of their activities related to SEFE.

2. Requirements for the organization of information security

- 2.1** The Service Provider appoint a competent contact person as a contact person on the subject of information security, if required.
- 2.2** The Service Providers design processes and perform tasks for SEFE in compliance with the principles of separation of functions, need-to-know and least privilege where appropriate and necessary.

3. Information security requirements for personnel deployment

The Service Provider shall ensure that:

- 3.1** The personnel employed by Service Provider or work for Service Provider are at least generally bound to secrecy.
- 3.2** Personnel working for the Service Provider who no longer need access to information and systems of Service Provider no longer have any access possibilities granted.
- 3.3** Personnel employed by the Service Provider or work for the Service Provider removes or copies project-related data without authorization.
- 3.4** The personnel employed by the Service Provider or work for the Service Provider return all devices and information properly and delete existing copies if the employment relationship is terminated or if no activities are performed for SEFE anymore.

4. Requirements for management of information assets

With regard to the management of values, the Service Providers shall ensure that:

- 4.1** SEFE's assets are not removed from SEFE's premises without prior approval.
- 4.2** Company information is logically processed and stored separately from third party information.
- 4.3** Upon completion or termination of work for SEFE, all copies of the Company Information, including all backup and archival copies, in electronic or non-electronic form, are purged and securely destroyed (or returned to SEFE upon request; exceptions are possible in case of

legal requirements). Upon request by SEFE, evidence of the secure destruction must be provided with relevant details (what, when, how, who, witness, if applicable).

5. Access control requirements

Within the scope of the access control to the Company Information, the Service Providers shall ensure within their area of responsibility that:

- 5.1** Devices are connected to SEFE's infrastructure only after approval by SEFE.
- 5.2** Devices connected to SEFE's infrastructure are equipped with up-to-date malware protection and are kept up-to-date with regard to security and function updates.
- 5.3** Before introducing an external data carrier into the infrastructure of SEFE (e.g. USB, CD, DVD, external hard disk) a prior check for malware is performed.
- 5.4** Remote access to SEFE's infrastructure is performed exclusively via communication channels and technologies approved by SEFE in advance (e.g. VPN, dedicated line, two-factor authentication).
- 5.5** Electronic systems on which company information is processed, stored or transmitted have appropriate access and identity management in accordance with the state of the art.

6. Physical and environmental security requirements

Service Providers shall ensure that the rules laid down on the part of SEFE for entering the Company's premises are strictly followed.

7. Requirements for operational safety

- 7.1** Information systems of Service Providers that are permanently connected to SEFE's infrastructure must ensure the following:
 - (a) Audit-proof logging of security-relevant user actions with a retention period of at least 90 days;
 - (b) Up-to-date malware protection;
- 7.2** Vulnerability and patch management.
- 7.3** SEFE shall be informed about existing or potential availability restrictions of the information systems under the management of the Service Provider, unless otherwise regulated.

8. Communication security requirements

- 8.1** Company information stored, processed or transmitted on systems or data carriers shall be protected in accordance with the state of the art (e.g. encryption, use of firewalls, etc.).
- 8.2** Rules regarding the classification and handling of information must be strictly observed. Specifications regarding the correct handling of classified information can be found in Appendix A.

9. Information security incident handling requirements

9.1 Service Providers shall have processes in place that allow for an appropriate handling of security incidents in the context of their organization.

9.2 Security incidents or vulnerabilities at the Service Providers, where impacts on SEFE cannot be excluded with certainty, shall be reported immediately to the contact person at SEFE or to infsec-global@sefe.eu.

10. Requirements on compliance

Upon request by SEFE, the Service Provider must demonstrate compliance with the security requirements described in this document by means of an appropriate audit conducted by SEFE or its agents or by other suitable means (e.g. evidence of ISO27001 certification with relevant scope).

Appendix A: Table for classification handling

How to label information

Information classified as **PUBLIC** does **not require a label**. However, it is strongly recommended to label as PUBLIC those document types (e.g. presentations) that have been approved as defined in this Policy and are presented at public forums and meetings. That makes it obvious that this information may be distributed.

This information must be explicitly authorised for publication by the public affairs division or other department(s) / person(s) authorised by the company management of SEFE.

The information owner is required to obtain this authorisation. Without this authorisation, all non-labelled information is to be considered classified as INTERNAL.

Please note that using information in public presentations etc. involves special requirements regarding format (corporate identity) and content.

The following rules are set out for classifying soft or hard copies of documents:

INTERNAL	CONFIDENTIAL	STRICTLY CONFIDENTIAL
Implicit	Always label as CONFIDENTIAL [company name] in bold and capitals on every page of document in header Include page number and total number of pages in footer: "page X of Y"	Always label as STRICTLY CONFIDENTIAL [company name] in bold and capitals on every page of document in header Explicitly list all recipients on page one of document Include page number and total number of pages in footer: "page X of Y"

How to handle information

- Please be aware that storing and processing of SEFE Group information by SEFE Group employees is only allowed on/in services provided by the IT-department or officially announced third party services approved by Global Corporate Security SEFE Group. Processing and storing information on private devices (if not additionally secured by solutions administrated by IT e.g. Blackberry Works, Citrix / myPortal) is prohibited.

What	INTERNAL	CONFIDENTIAL	STRICTLY CONFIDENTIAL
Duplicating using a copier or printer	Retrieve originals and copies from the copier or printer as soon as possible Copies, printouts and scans must not be produced on publicly	Copy, print, and scan processes must be supervised (e.g. print out after entering PIN or validation with ID-Card)	With approval from the information owner only. Copy, print and scan processes must be supervised (e.g. print out after entering PIN or

	accessible equipment	Producing copies, printouts and scans on publicly accessible equipment is prohibited	validation with ID-Card) Producing copies, printouts and scans on publicly accessible equipment is prohibited
Transferring information	Information may be forwarded to all Company employees and third parties where it is generally required for their work	Information may be forwarded upon the information owner`s request to Company employees and third parties who have signed Confidentiality Agreement for their work at SEFE Group Alternatively, the information owner may explicitly determine who has access to this information (either by name or by role)	The information owner must explicitly determine by name persons who can receive and store the information
		Further disclosure of information classified as CONFIDENTIAL or STRICTLY CONFIDENTIAL is possible only after prior written consent of the information owner who initially transferred this information and defined the number of persons who have access to it.	
		The disclosure of CONFIDENTIAL/STRICTLY CONFIDENTIAL information in a tangible form (i.e. in hard copies or on electronic devices) must be conducted issuing the appropriate acceptance certificate signed by the authorised representatives of the parties. The template of this acceptance certificate is attached to this document in Annex B	
Communicating information externally (for example, to the press or government authorities)	Always obtain approval from the public affairs division or other department(s) / person(s) authorised by the company management.		
Presenting information at conferences (externally)	Approval of Public affairs division or other department(s) / person(s)	Prohibited	

	authorised by the company management is required	
--	--	--

What		INTERNAL	CONFIDENTIAL	STRICTLY CONFIDENTIAL
Sending by email	Internal	Ensure that the recipient's address is correct (must be company address)	<p>Ensure that the recipient's address is correct (must be company email address), the recipient must be admitted to this information</p> <p>Indicate the confidentiality class via categorisation function in the email programme or alternatively label the subject of an email</p>	
	External		<p>Ensure that the recipient's address is correct (must be company email address)</p> <p>Email text and attachments must be encrypted. In case there is no email encryption solution in place, put the confidential or strictly confidential information in an encrypted ZIP-File and attach it to the email. The password must be transferred via a different channel (SMS, phone call, etc.)</p> <p>Indicate the confidentiality class via categorisation function of your email programme or alternatively label the subject of an email</p> <p>Note: Instead of an encrypted email, the following alternatives can be used: secure data transfer platform managed by SEFE Group like HUBSTER or myBox</p>	
Sending by post	Internal	Information can be sent in unsealed internal mail envelopes	Information must be sent in sealed envelopes protecting it from unauthorised access marked CONFIDENTIAL Envelopes must be marked "Upon delivery in person"	Information must be sent in sealed envelopes protecting it from unauthorised access marked STRICTLY CONFIDENTIAL Envelopes must be marked "Upon delivery in person"
	External	Send the information in a normal letter	Send the information in tamper-proof envelopes Use acceptance certificate (Annex B)	Send the information in tamper-proof envelopes by registered letter with

			personal delivery or by courier Use acceptance certificate (Annex B)
			Tamper-proof envelopes: two envelopes are to be used. The inner envelope must be tamper-proof and feature a label of the confidentiality class, while the external envelope must not indicate the confidentiality class
Sending by fax	Internal	Ensure that the recipient's number is correct	Prohibited
	External	Ensure that the recipient's number is correct. Use a cover page that specifies the number of pages	Prohibited

What	INTERNAL	CONFIDENTIAL	STRICTLY CONFIDENTIAL
Destroying information stored on paper	Office waste-paper baskets	The documents must be destroyed in document shredders. Destruction of documents can be carried out by a special contractor. For these purposes special sealed containers can be provided on each floor at the office for collection of information.	Securely destroy documents using document shredders.
Verbal distribution	Permitted only when no unauthorised persons can listen in. Confirm the identity of the person you are talking to.		
Storing information in IT applications	Store information to applications in accordance with their classification and taking account of access authorisations; if necessary, assign access authorisations explicitly.		
Storing information on Fileserver	Store on drives and folders available, taking account of access authorisations; if necessary, assign access authorisations explicitly	ADDITIONALLY, information must be stored in encrypted folders (e.g. data safe, encrypted container). In case there are no encrypted folders available, use encrypted ZIP files or folders with explicit access authorisation. The information owner must regularly monitor access rights.	ADDITIONALLY, information must be stored in encrypted folders and the information owner must regularly check access authorisations (e.g. data safe, encrypted container) In case there are no encrypted folders available, using encrypted ZIP files or folders with explicit access authorisation is also possible. The information owner must regularly monitor access rights.
Storing information on mobile devices (laptops, mobile phones, etc.)	Only use devices/services provided by IT (e.g. blackberry work)		
Storing information on portable storage media (CDs, DVDs, USB sticks)	In common cases, all data should be encrypted.	Data must be encrypted. Right after completing the task, the data should be deleted from the portable storage device.	

	Right after completing the task, the data should be deleted from the portable storage.	When portable storage device is not in use (or left unattended), it must be kept in a lockable drawer or safe.
Deleting electronic information from storage media	Operation system-specific command or program tool should be used	To clean the media, specialised software that provides multiple overwrites of the used storage areas should be used
Disposing of portable storage media (CDs, DVDs, USB sticks)	Physically destroy the storage media	Hand in the storage media at local workplace team to be securely destroyed
Publishing information on the Internet	Prohibited	
Using web services, cloud services, free web space, etc.	As an exception only and only after a documented risk analysis has been prepared and approved by the Global Corporate Security SEFE Group	Prohibited