Sval

Acceptable Use Standard

1.0 Purpose and scope

The Acceptable Use Standard supports secure business continuity and growth by outlining safe use of Information and Communications Technology (ICT) systems, as inappropriate use exposes Sval and our employees to risks including.

- loss or theft of personal ICT equipment or information
- theft or unauthorized disclosure of authentication details
- unauthorized disclosure of personal data
- compromised information systems, such as any malware infections or hacked accounts
- reduced efficiency and lost opportunities, and
- legal issues and financial loss

Compliance to this standard safeguard that our performance and communication meet the high standards for Information Security that we want our business and people to be recognized for – and which are fundamental for our future success.

This standard applies to all users of Sval's Information and ICT systems, whether accessed using Sval equipment or non-Sval equipment. All users are responsible for exercising good judgment regarding appropriate use of Information and ICT systems in accordance with Sval policies and governing documentation.

Violations of the principles and responsibilities in this Standard may lead to disciplinary action as stated in our working regulations ("Arbeidsreglement") or any contractual agreement.

2.0 General principles, ownership, and rights

- Sval's information systems, including personal computers, mobile phones, networks, storage and processing systems, cloud services, e-mail, internet browsers, etc. are the property of Sval and shall be used securely for business purposes in serving the interests of the company.
- Sval's proprietary information stored on electronic devices remains the sole property of Sval. The users of such devices and Sval as a company must ensure protection of information in accordance with Sval policies and governing documentation.
- Sval is responsible for the security and performance of information systems. Sval uses systems monitoring to identify performance-, cost- and security risks, including detection of unauthorized and unacceptable activity.
- To reduce risks and following changes in business needs, Sval has the right to pause, change or terminate end-users' access to services.
- In response to threats, Sval has the right to delete accounts and data to ensure proper service operations or to safeguard information. Sval has NO responsibility for private data that could be lost in this scenario which may include remote wipe of user devices.
- At the last day of a user's engagement, the user´s accounts will be deactivated. However, it can be legitimate to keep the email account active for a limited period to ensure that significant information is not lost. The active account of a former user will be used only to receive emails. The email account will then be finally closed, as long as there are no other particular circumstances qualifying further storage. and content deleted
- Data stored on Sval servers, including cloud data stored on Microsoft Office 365 such as SharePoint and OneDrive are backed up periodically, to Sval dedicated backup systems, to ensure the availability of data in case of system or data loss. This does NOT include data stored locally on users' devices.

3.0 Privacy

Sval will comply with the Norwegian privacy act (“Personopplysningsloven”). All processing of personal data will be in accordance with a defined lawful purpose.

As a general principle, Sval will NOT open, search or read personnel´s mailboxes or other storage media. This principle can be overridden only if it is necessary for restoring Sval’s daily operations, for security reasons or by legitimate orders of the Norwegian police, National Security Authority or other relevant public authority. Any inspection must be approved by owner of this Standard and at any time comply with relevant legislation and governing documentation within Sval.

A Sval user account with access to Sval systems and networks, will hold the following personal data: username, full name, position title, work email, mobile number as well as reporting lines and access levels.

If Sval’s follow-up of obligations stated in this Standard requires processing of personal data regarding personnel, such data will be handled in accordance with relevant company guidelines, incl. our code of conduct and the Norwegian privacy act (“Personopplysningsloven”).

4.0 Instructions for use

4.1 General

- You have a responsibility to promptly report incidents, suspicions and vulnerabilities to the IT ServiceDesk, Information Security responsible and/or your immediate manager. Examples include loss or theft of equipment, information and authentication details.
- You may access, use or share Sval information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- If you have technical access to information that you are not authorized to access within your organizational duties and/or responsibilities, you must immediately report this to the IT ServiceDesk and/or your immediate manager.
- You have a responsibility to protect the confidentiality of information accessed and displayed on your screen.
- You have a responsibility to protect the confidentiality of information accessed and displayed on your screen.
- You have a responsibility to protect personal ICT equipment from being taken or accessed by unauthorized personnel. You shall assess the need for securing equipment when leaving your workplace for the day.
- All business-related information and data are to be stored on the designated central storages provided by Sval. Storage of business critical or sensitive company information on personal ICT equipment shall be avoided. If necessary, such information shall be encrypted.
- Sval systems and information can only be accessed and handled digitally using safe and relevant end-user equipment. Such equipment includes.
    - Sval issued personal laptops and smartphones
    - Contractors' personal laptops and smartphones
- You are responsible for exercising good judgment regarding reasonable private use of Sval’s information systems. If there are any uncertainties, you are to consult your immediate manager.
- Private data on company systems are to be stored in separate private folders and clearly marked. The company has no responsibility for private data stored on company systems and equipment.
- When disposing personal Sval ICT equipment, the unit memory and storage shall be professionally erased or destroyed. Return equipment to or consult the IT ServiceDesk.

4.2 ICT systems use and security

1. Only electronic devices that are provided by Sval can connect to the internal corporate network (office network).
2. Any non-Sval provided and managed equipment shall only be connected to the guest network.
3. Storing Passwords in browsers should be done with utmost care and is prohibited for systems containing information that is classified or should be understood as sensitive or confidential.
4. All devices with access to Sval systems and information must be secured with an automatic password-protected screen lock set to 5 minutes or less. Mobile phones must be automatically locked within 5 minutes with a minimum 6-digit pin code or other secure authentication (i.e. fingerprint or face recognition).
5. Password-protected screen lock are enforced on Sval managed devices such as mobile phones and computers. When leaving your device with access to Sval's systems and information unattended, you shall ensure that your device is secured properly, i.e., turn off, log off, screen lock etc. This including leaving your office desk for any reason.
6. Do not download software from the internet or execute or accept any software programs or other code on the internet on Sval ICT equipment unless it is approved by the Sval.
7. Regularly or automatically update your devices (i.e. smartphones, tablets and computers) from trusted sources, i.e. google play or apple app stores, or any Sval managed software update service.
8. You must use caution when opening attachments or accessing links received on email, as they may contain malware. Contact the sender and/or IT ServiceDesk if you are in doubt.
9. It is not allowed to move or copy data using a USB storage device (memory stick, external hard drive etc). Sval has enforced a requirement to block USB storage devices on Sval PCs for all users. If you do have a business-critical requirement to use USB storage to move data, please reach out to Sval IT ServiceDesk in order to get assistance with this.

4.3 Electronic messaging and remote work and travel

1. Sval confidential or proprietary information, or sensitive personal data shall to the extent possible be shared through Office365.
2. Tools for electronic messaging and collaboration is provided by Sval, our partners and trusted vendors and include email, MS Teams and cellular services (SMS and voice). Other messaging services should not be used for communicating confidential information.
3. All work outside Sval premises is defined as remote work. When using private and trusted networks for work, e.g. work from home, take precautions in reducing risk of infections from other devices by:
    A. Ensuring devices' software stay updated
    B. Ensuring devices' passwords are changed from factory default
4. Use of public or other insecure wireless networks should be avoided. Instead, you should use password-protected internet sharing from your own mobile or internal simcard.
5. When working in public areas, privacy screen protectors should be used. Avoid use of publicly available USB chargers, i.e., in airports and hotels or on public transportation, incl. airplanes, trains and buses.
6. Personal ICT equipment shall not be left unattended and unsecured in public or other areas which should be understood as available for violators.

7. When traveling, equipment containing information classified as confidential or higher shall be handled as hand luggage, incl. laptops, mobile phones, external drives and documents.
8. When traveling abroad, please note that some countries may require encrypted equipment to be decrypted to perform control. In such cases, encrypted material shall not be taken to such countries.

4.4 Social media activities and personal data

1. Limited and occasional use of Sval's systems to engage in social media is acceptable, provided that it is done in a professional and responsible manner.
2. All social media activity using Sval's systems or as long as you can be perceived as a representative for Sval (e.g. stated employment in private user profile or use of the company logo), must not violate the terms and restrictions in this Standard, our Code of Conduct, policies, confidentiality clauses, or otherwise damage Sval's good reputation or best interest.
3. Posting from an Sval email address or use of Sval title or account, to public sites shall only be done by authorized personnel. If you are not sure what will be appropriate use of social media, consult your immediate manager for advice.
4. All handling of personal data in Sval systems or services that are required for work-related purposes, shall be carried out in accordance with relevant company guidelines, incl. our Code of Conduct and the Norwegian privacy act ("Personopplysningsloven"). This also applies to disclosure of personal data within Sval.

5.0 Unacceptable use

The Acceptable Use Standard applies for all use of Sval systems and equipment, including breach of applicable laws and regulations and Sval policies and governing documentation.

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities or by specific authorization. The list under is by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.
General activities, system and network activities and personal data:

1. Violations of copyright protected rights of any person or company, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by Sval
2. Exporting software, technical information, encryption software or technology, in violation of export control laws, is illegal. Consult the appropriate management prior to export of any material that is in question.
3. Using Sval computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
4. Making or accepting fraudulent offers of products, items, or services.
5. Sending unwanted email messages, including the sending of “junk mail” or other advertising to individuals who did not specifically request such material (email spam).
6. Any form of digital harassment, whether through language, frequency, or size of messages.
7. Creating or forwarding chain letters, “pyramid or multi-level marketing” schemes or any attempts of fraud or misleading encouragement to investment.
8. Deliberate introduction of malicious programs or exploits on any information systems, incl. remote access software, spyware, crypto-viruses, worms, trojans, cryptocurrency miners, etc.
9. Storing passwords in clear text, revealing your account password to others or allowing use of your account by others. This includes family and other household members.
10. Intentional effecting security breaches, disruptions of network communication or network monitoring of traffic not intended for your host, unless these duties are within the scope of regular duties and approved by the information security responsible. Security breaches include, but is not limited to, accessing data of which you are not an intended recipient or logging into a server or account that you are not expressly authorized to access. “Disruption” includes, but is not limited to, network sniffing, pinged floods, port- or security scanning, packet spoofing, denial of service and forged routing information.
11. Circumventing user authentication or security of any host, network or account.
12. Unauthorized use, or forging, of email header information.
13. Providing information about or lists of Sval personnel to parties outside Sval is prohibited unless authorized or part of the employee’s normal duty or done as part of Sval legal obligations or contractual fulfilments. Sharing business contact details for business purposes is permitted.