Policy on information security in connection with supply relationships

– in short: IT security policy for suppliers –

Contents

1. Scope of application

(1.1.) This policy applies to all employees of the Schütz Group and their suppliers that are involved in IT services. IT services comprise all forms of IT supply. This includes for instance the provision of IT systems, projects/trades or the provision of personnel. It comprises outsourcing or other external procurement of IT services. In addition to employees of the IT and purchase department, this also includes the employees responsible for the procurement or IT of all departments of Schütz, those of the suppliers and of their sub-suppliers. The confidentiality class is defined in the “Non-disclosure agreement” (NDA).

2. Objective and subject matter of this policy

(2.1.) The objective of this policy is to protect the corporate values of the Schütz Group that are accessible to suppliers. This includes safeguarding of the protective goals (confidentiality, integrity and availability) of information security, in order to prevent security risks.

(2.2.) The policy on information security in connection with supply relationships deal with some fundamental aspects in terms of information security and data protection that become essential if Schütz performs IT procurement processes in collaboration with suppliers. This policy is a supplement to the general operational regulations on information security and data protection and explicitly extend the scope by the companies functioning as suppliers for the Schütz Group. This policy does not replace the NDA.

(2.3.) A prerequisite of procurement will be that this policy is provided to the supplier and checked prior to any business transaction. Written confirmation of the supplier regarding the receipt of the document and consent of the contents will be required in any case.

(2.4.) The supplier undertakes to provide immediate and effective protection, in the context of the current state of the art, to all information and data, in accordance with the specified information security measures of Schütz.

3. Information security measures

(3.0.) In the following subsections, the applicable rules for suppliers/service providers will be defined. The prohibition signs indicate impermissible conduct. The warning signs serve to provide information and create awareness. The mandatory signs define instructions.

3.1. Prohibition signs 

(3.1.1.) Access to mobile removable storage devices (USB stick, disks, SD cards, CD/DVD, etc.) is to be avoided. The use of data carriers supplied by Schütz is permissible. USB interfaces are locked on the system side by default. If USB use requires sharing, the employee from Schütz has to request this use via the internal HelpDesk system. For external data transmission processes, use https://share.schuetz.net/. The transfer of confidential/strictly confidential data is only permissible by encryption via “share.schuetz.net”.

(3.1.2.) All user accounts are provided with password protection by the system. Users have to change their password every 90 days. This password expiration must not be deactivated. Specific system users, communication users, service users, collective users or production users are exempt from this password expiration. Passwords must not be stored on the components in plain text or in writing.

(3.1.3.) Any network equipment, e.g. switches, routers, access points, firewalls, etc. shall be provided by Schütz without exception. Network services such as DNS, DHCP, WINS, PXE or the like may only be started up or operated in the internal Schütz network upon consultation with the IT department. In duly substantiated exceptional cases, the use of network devices operated by the supplier can be checked and approved by the IT department.

(3.1.4.) The disclosure or provision of data or information vis-à-vis third parties (e.g. family members) is not permissible. Sharing or access (e.g. when working from home) by third parties is not permitted either.

(3.1.5.) Regular printing in the Schütz network to the floor printer is not permissible. When printing, “confidential” printing must be selected. The unauthorised taking of pictures is not permitted.

(3.1.6.) Refrain from unencrypted communication. Data encryption is always mandatory if data or applications requiring protection are accessed by insecure media (e.g. Internet). For the encryption, neither use insecure or weak encryption algorithms and key lengths nor encryption algorithms and key lengths that are already compromised. Always set up the strongest encryption algorithm and the most secure key length. If this is not possible, contact IT Security.

(3.1.7.) The software or hardware used by the manufacturer must be maintained and updated using technical or organisational means. Exceptions shall be evaluated separately by the IT Security department.

(3.1.8.) When working on new components or components already in use, insecure configuration must not be left. Configuration must be carried out in compliance with the state of the art.

(3.1.9.) Using your own equipment is not permissible. If the necessity of utilising personal equipment should arise, the IT department must give its consent.

3.2. Warning information 

(3.2.1.) All access processes will be logged for purposes of monitoring and compliance. Dial-in, login and logout data as well as access data (user name, date, time and login/logout) will be logged centrally**.** Schütz reserves the right to store all log data in accordance with the valid, internal company agreement. This includes Internet access, remote access processes, login and logout processes, email transfer processes, etc.

(3.2.2.) Connections to systems, logged-in users and tasks and transactions executed will be stored in the framework of constant, automated monitoring. Evaluation will take place ensuring data protection. Separate regulations shall apply to tasks on the plant premises.

(3.2.3.) Remote access cannot be freely selected. Schütz offers the following types of remote access:

- WatchGuard Mobile VPN via SSL for individual remote access from a computer outside the internal network.
- Cisco Webex or TeamViewer is provided for spontaneous support, for example remote control or remote maintenance of computers.

(3.2.4.) The service provider commissioned shall be able to identify himself/herself for the assignment at all times by presenting an ID card or a document signed and issued by the supplier. The ID card or the signed document must be presented by the service provider without being asked to do so before receiving the visitor badge, and it must be produced on request. If this policy is disregarded intentionally or negligently, this may lead to a ban from company premises.

(3.2.5.) Visitors must be supervised during their stay and shall only gain access to the areas essential to their stay. With the “What to do in the event of an emergency” section, the security requirements in the event of an emergency will be communicated.

(3.2.6.) The staff shall ensure that third parties merely receive information on a “need-to-know” basis for tasks/activities within sensitive areas. They shall be provided with as much information as needed to perform the task in question.

(3.2.7.) Access from the Schütz network to the Internet can also be established via the guest network. The application required for this purpose can be made by employees from Schütz via the visitor administration function or directly at the reception desk.

(3.2.8.) It has to be ensured that only devices and components secured in accordance with the state of the art will be used for maintenance and configuration.

(3.2.9.) Legal and regulatory requirements, including data protection, intellectual property and copyright shall be complied with. For support requests, in the event of faults, problems or incidents, the Schütz IT HelpDesk is to be notified.

(3.2.10.) To ensure proactive planning and design of IT components, they have to be clarified with the IT department before being procured or commissioned. In this way, compatibility, among other things, is ensured.

3.3. Mandatory information 

(3.3.1.) The suppliers' IT contact persons are to be designated while orders are initiated: IT expert responsible, IT sales department, IT Security/information security officer. In the "Responsibility and contact persons" section, the roles mentioned are specified by name. If the roles mentioned are not specified, appoint the persons responsible.

(3.3.2.) Offers, order confirmations, invoices and other documents with IT components are to be disclosed in detail. This includes clear specification as to the manufacturer, model, edition, version, license metric, generation, quantity, currency, itemised costs, etc. In the case of software components, licensed and software maintenance are to be separated. For project prices or discounted prices – if possible – nevertheless the individual prices of the deliveries or services are to be shown. Maintenance or support services are to be itemised separately.

(3.3.3.) If possible, Schütz will provide the client or server hardware including the initial operating system installation by an automated and standardised process. Windows computers shall be integrated into the domain and receive virus protection. External network components may only be used to access internal network resources with the explicit approval of Schütz IT.

(3.3.4.) Any software used on clients or servers must be reported to the IT department. Depending on the degree of utilisation, the software to be used shall be centrally packetized by Schütz. This is to be coordinated with the Schütz IT department.

(3.3.5.) All digital users for external employees have to be applied for by the responsible Schütz employee via the Schütz-internal helpdesk system. The approval of administrative rights (Windows administrator, Linux root or Microsoft SQL et cetera) will only be permissible in justified individual cases and exceptional cases, for example for installation or commissioning processes or comparable scenarios. Access rights will be granted restrictively.

(3.3.6.) Daily operation of the systems always has to be ensured without administrative rights. Computers and mobile devices must be protected against unauthorised use by means of key lock or the like, e.g. password protection, whenever they are not in use. All suppliers, visitors and other third parties must wear the provided visitor badge so that it is clearly visible.

(3.3.7.) The authentication of systems or solutions should be linked to the central Microsoft Active Directory of the Schütz Group. Decentralised user administration is to be avoided and has to be coordinated with the Schütz IT department.

(3.3.8.) Any access data (user name, passwords, codes, PINs, etc.) must be treated confidentially. This also includes physical keys or access chips (Legic, RFID, etc.) The clean-desk rule is to be applied. Upon completion of the assignment, physical means of access (e.g. chip, key, etc.) are to be returned.

(3.3.9.) The supplier undertakes to comply with and observe all data protection regulations in the version applicable at the time in question. The supplier undertakes to instruct all employees as to the data protection regulations applicable in each case and to place them under the obligation to maintain data secrecy. These explanations are to be presented to the data protection officer from Schütz on request.

3.4. What to do in the event of an emergency

If you suspect a virus infection or the like, stop working and report your suspicions to the IT helpdesk. Do not implement any measures without instructions by the IT department. Memorise all suspicious features well and document them. If you have noticed a breach of data privacy, additionally contact the data protection officer.

1.) Keep calm! Uncoordinated action may destroy valuable evidence.

2.) Disconnect the device from the network. This implies the wired and the wireless network. The IT department will support you if you have any problems.

3.) Do not shut down the device and do not switch it off! Otherwise you may destroy valuable volatile analysis data. An employee from the IT department will save these data.

4.) After the data backup, the device can be switched off. The device will be collected by the IT staff for further analysis and backup.

5.) The device will undergo re-installation and required programs and data will be restored.

IT emergency contacts:

IT help desk:

Hotline: +49 2626 77955
E-Mail: helpdesk@schuetz.net
Portal: helpdesk.schuetz.net

Service hours: Monday - Friday 7 am - 6 pm
IT on-call service outside these service hours: +49 2626 77-1331

IT Security department - e-mail: itsecurity@schuetz.net

Head of IT Security Sven Westenberg:
Office: +49 2626 77-419 / +49 2626 77-18419
Mobile: +49 1752 286592
E-mail: sven.westenberg@schuetz.net

Gatekeeper (Selters):
Contact: +49 2626 77-260

Data protection officer Christian Baier:
Office: +49 2626 77-740
E-mail: datenschutz@schuetz.net

4. Obligation and persons to contact

4.1. Obligation to comply with the “Policy on information security in connection with supply relationships”

The supplier has read and understood this policy and agrees to the content and his/her obligations. Furthermore he/she ensures that his/her employees commissioned as well as sub-providers have been instructed with regard to this policy. Instructions as to the conduct in the event of an emergency have been given in this document.

_____

(Version of these policy)

_____

(Company)

_____

(Street, postcode, town)

_____

(Title, surname, first name)

_____

(Place, date, signature)

4.2. Contact person of the company stated above: (see item (3.3.1.))

_____

_____

(Surname, first name, role) (E-mail address, telephone number)

_____

_____

(Surname, first name, role) (E-mail address, telephone number)

_____

_____

(Surname, first name, role) (E-mail address, telephone number)

_____

_____

(Surname, first name, role) (E-mail address, telephone number)

5. Revision table

No.	Date	Version	Name/department	Change description
01	27/04/2022	V1.0	Wika von Czarnowski, David / IT Security	Initial creation of the document
02	02/05/2022	V1.0	Wika von Czarnowski, David / IT Security	Finalisation after internal clarification
03	22/02/2023	V1.0	Sven Westenberg / IT Security	Short name, information classification
04	14/11/2023	V2.1	Steven Beck; Sven Westenberg / IT Security	Annual revision with edito-rial changes. NAC passage added.