Cybersecurity
Rules for Business Partners

Date: 2021-03-12, Version: 1.1
Published by: CYS GRS RM
Unrestricted

1 Scope and Applicability

The Rules for Business Partners apply to business partners of Siemens who have access to IT systems, applications, networks, or to any Content[1] business partner has access to due to a contractual relationship.

The defined rules and principles herein apply independently whether the business partner uses IT systems of Siemens or its own IT systems, if the business partner works in a Siemens office or not, or if a connection to IT resources of Siemens is set up (e.g. to an IT system or an IT application).

For the avoidance of doubt, the Cybersecurity clauses of an underlying agreement shall remain applicable.

1.1 Responsibilities

The business partner of Siemens is granted access to IT systems, applications, networks or Content to fulfill its contractual obligations and to increase the efficiency of business processes.

This requires measures for the protection of IT systems, applications, networks, and Content to prevent unintentional disclosure, unauthorized access, manipulation, computer viruses, hacking, cyber-attacks and other IT security threats. For that purpose, it is necessary that business partners of Siemens comply with the following rules and principles and that protective measures are not deactivated, circumvented or changed in any other way, all such measures in consistence with state-of-the-art Cybersecurity standards (e.g. ISO 27001).

The business partner shall comply with the herein defined rules and principles in addition to the contractual agreement and to bring this document to attention and consistent adherence to its employees and any subcontractors who have access to IT systems, applications and networks of Siemens or receive Content.

In this policy, the term “business partner” is used throughout to refer to business partners and their employees.

1 Content shall mean information or data (not in the public domain) obtained, generated, exchanged, collected or stored based on all kinds and formats, including digital format (e.g. data stored on electronic or optical media), or physical (e.g. paper), numerical, audiovisual, graphical, cartographical, narrative or in intangible format (e.g. know-how), either owned by Siemens or processed on behalf of its customers and suppliers and accessible for business partner.

SIEMENS

The business partner is obliged to adhere to the guidance and regulations of Siemens for the security of IT systems, applications, and networks.

In case business partner employees are fulfilling their contractual obligations remotely (neither on Siemens nor on business partner premises), business partner shall ensure that its employees also adhere to business partner's state-of-the-art remote working policies in addition to the requirements stipulated in this document and the underlying agreement (e.g. via awareness trainings for securely working from home).

2 Rules and Principles

2.1 Training of Business Partner Personnel

To fulfill the contractual obligations, business partner shall only engage personnel educated in state-of-the-art information security (and secure coding, where applicable) and ensures to upgrade their knowledge on a frequent basis (at least once per calendar year).

Business partner personnel engaged by Siemens shall make themselves familiar with Siemens' information security policies, standards and guidelines and shall attend information security trainings, if requested by Siemens.

Business partner shall inform Siemens in advance if personnel shall be replaced in fulfilling the contractual obligations.

2.2 Handling of Content

Business partner shall adhere to and make use of the communication and collaboration solutions for Information exchange provided by Siemens (see "Secure Communication and Collaboration with Siemens"), if not agreed otherwise between the parties.

Any form used to conceal, distort, or forge the identity or the meaning of Content by the business partner is prohibited.

2.2.1 Protection of Content

Regardless of the form in which it appears, or the information medium employed, all Content must be protected in accordance with its level of classification of confidentiality, integrity, and availability.

For Content owned by Siemens there are three protection classes: "Restricted", "Confidential" and "Strictly Confidential". In relation to the protection classes, the identification/creation, distribution, dispatch and transmission, retention and storage as well as disposal/destruction/deletion shall comply with measures that are more stringent as the need for protection increases.

The business partner defines the level of confidentiality of the Content it creates in consultation with its respective contact at Siemens. The business partner is obliged to comply with the protection measures defined by Siemens for the Content entrusted.

Content shall only be stored and processed on IT systems, applications and file storage systems that guarantee an adequate protection of the information, i.e. Content with protection classes "Confidential" shall be stored and processed encrypted and for "Strictly Confidential" shall be encrypted end-to-end.

The business partner shall neither produce copies or reproductions of Content, nor delete, examinate, or modify such Content without the prior consent of Siemens or unless contractually agreed otherwise between the parties.

2.2.2 Transmission of e-mails

Secure e-mailing pertains to e-mail correspondence originating from or between business partner's employees and contractors, IT systems, applications, and Siemens.

E-mails, which must guarantee the integrity and the level of confidentiality of the Content and the identification of the sender, including but not limited to:

- e-mails with commercial or legal impact
- e-mails which require user interaction
- e-mails which are related to critical security services
- e-mails which contain potential malicious content (e.g. URLs, attachments)

shall be, in adherence to state-of-the-art standards (e.g. NIST SP800-177R1, TN-1945 or BSI ISi-Mail-Server), digitally signed and transmitted in encrypted form end-to-end for Content with protection classes "Confidential" or "Strictly Confidential" (e.g. using the S/MIME standard http://www.siemens.com/digital_id_en; please refer to "Secure Communication and Collaboration with Siemens").

The automatic forwarding of incoming e-mail to external mailboxes, e-mail spamming, misuse of Siemens e-mail addresses (e.g. adding e-mails to mailing lists without explicit consent) is prohibited as well as the transmission of confidential or strictly confidential Content via fax.

2.2.3 Deletion of Content

The business partner shall delete reliably all Content from all its information media which is not or not any more of relevance for the provision of the contractually agreed tasks or activities, except retention is contractually agreed or required according to applicable laws and regulations.

Content stored in electronic or paper format shall be deleted, sanitized and disposed depending on its level of confidentiality (i.e. Content with protection classes "Confidential" or "Strictly Confidential" irretrievably) in adherence to state-of-the-art standards (e.g. BS EN 15713 – protection level 6, NIST SP800-88, DIN 66399-2).

2.3 System Access and Admission Authorizations

If required and not otherwise agreed between the parties, business partner shall access Siemens' network and Content solely by Siemens provided access solution depending on the protection level of the respective IT system, application and network (e.g. via Siemens' business partner access solutions).

Business partner shall log any of its access to Siemens and protect any connection between Siemens' intranet and its environment against access from third parties.

The business partner shall only exercise received system access and admission authorizations (e.g. password or access cards) for the fulfillment of its contractually agreed tasks and activities. Such system access and admission authorizations shall be restricted based on the principles of "least privilege", "need to know" and "segregation of duties".

Business partner shall timely inform Siemens in case of any changes of business partner's employees or subcontractors having access to Content.

The admissions, all related technical configuration or cryptographic material shall be kept confidential and shall be neither shared with any third party nor made public.

The business partner shall not circumvent or misuse such access solution and related security mechanisms.

2.4 System and Data Access Protection

IT systems and information media used by the business partners or provided by Siemens to fulfill their contractual obligations must be protected against unauthorized access, including physical security for business partner's working environment, via state-of-the-art measures.

2.4.1 IT systems and information media provided by Siemens

IT systems and information media provided by Siemens are secured and regularly monitored based on Siemens rules and regulations and such security measures shall not be circumvented by the business partner (no manipulation or bypassing). Business partner shall handle such IT systems and information media with due care, including at a minimum the following protection measures:

- Making use of theft protection for mobile systems.
- No misuse or unauthorized access when sharing resources.
- Use of different passwords per user account (anonymous and guest access to be disabled).
- No elevating of access privileges without Siemens preceding approval.
- Switching off voice-controlled smart devices or any webcams in the working area not required for business purposes (e.g. Amazon Alexa, Apple Siri).
- Logging off and storing the devices securely if not in use.
- Paper documents containing confidential or strictly confidential Content shall not be openly accessible or left unsupervised. They shall be locked away with appropriate protection mechanisms.

2.4.2 IT systems and information media owned by business partner

In addition to section 2.4.1 the following measures are additional minimum protection measures for IT systems information media owned by business partner:

- Current Bios version installation and Bios password activation.
- No use of permanent local administration rights.
- Enabling screensaver with password protection of the operating systems (as system lock for unattended IT systems).
- Activation of hard disk and file encryption.
- State of the art protection against viruses and similar malicious software provided the IT systems or information media are subject to such risks. Current and permanently active virus protection must be used for PC systems, including an endpoint detection and response agent.
- Securing of network access via password as a minimum to protect against illicit and malicious network traffic (e.g. white listing).
- No use of standard passwords. Deletion of initial passwords after receipt and expiry after 24 hours.
- Passwords shall be created from a combination of uppercase and lowercase characters, numerals, and special characters. Passwords shall contain a minimum of 12 characters (26 characters for administrator accounts). For PINs arbitrary numerals shall be used. Passwords shall be changed every 180 days (45 days for privileged administrative accounts), except the password is part of a two-factor authentication. The last 10 passwords shall not be reused.
- For access to confidential and strictly confidential Content two-factor authentication is required.
- During access to Siemens IT systems and networks no additional internet connection of the device shall be accessible.
- No use of network or system analysis devices without the explicit preceding approval of Siemens.
- Network devices connected to and third-party software used on such devices must be under regular support and maintenance and business partner shall ensure to have their current patch level applied.

2.5 Information Obligation, Cybersecurity Contact, Monitoring

2.5.1 Information obligation

The business partner shall inform the defined contact persons by Siemens (incl. Cybersecurity contact, contract owner) about any operational disruptions, identification of faults and damage factors (e.g. computer viruses, program malfunctions) in all IT systems, applications, networks or software used in their collaboration.

In case the business partner identifies vulnerabilities or security incidents or any suspicion thereof, it will notify Siemens immediately, e.g. suspicion of misuse or disclosure of PINs/passwords.

2.5.2 Cybersecurity contact

Next to the respective Siemens contact persons, the following Siemens Cybersecurity contact addresses shall be immediately informed in case of any:

- security incident: cert@siemens.com
- security vulnerability: svm.ct@siemens.com

potentially or effectively impacting the breach of Content, IT systems, applications, networks or information media.

2.5.3 Monitoring

Siemens controls and monitors business partners' adherence to these rules and principles as described herein. IT systems connected to the networks of Siemens are checked for security vulnerabilities according to state-of-the-art methodology. Identified vulnerabilities must be remediated by the business partner without undue delay. All security relevant patches and hotfixes released by third parties in conjunction with the contractual obligations must be installed.

The business partner shall also log and monitor its compliance to the rules and principles set herein in a suitable manner, complying with applicable legislation (e.g. retention periods).

If the business partner disregards the rules and principles contained herein, this may result in disabling its access to Siemens sites and IT systems and may lead to the agreed contractual or legal consequences.

2.6 End of Business Relations

At the end of business relations with Siemens, including the end of business relations of a business partner's employee, and unless otherwise agreed or requested by Siemens, the business partner shall conduct the following activities and confirm in writing:

- Return of all IT systems, devices, Content, information media, paper documents and work equipment (incl. access cards).
- Return of all granted accesses and declaration of these accesses for the purpose of deactivation or deletion (e.g. access to file shares, service accounts, etc.).
- Deletion of Content on all information media and destruction of paper documents in accordance with section 2.2.3.
- Deinstallation of any software provided by Siemens for the provision of the contractual fulfillment (e.g. virtual client software).