SIEMENS

Charter of Trust

We are signing for Cybersecurity

Be aware, be secure

Cybersecurity

Rules for Business Partners

Date:	Apr-2026
Version:	1.4
Published by:	CYS GRM RM

1. Scope and Applicability

The Rules for Business Partners apply to business partners of Siemens who have access to IT systems, applications, networks, or Content[1] as the result of a contractual relationship with Siemens.

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

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

1.1. Responsibilities

The business partner is granted access to IT systems, applications, networks, and/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 comply with the following rules and principles and that protective measures are not deactivated, circumvented, or changed in any manner inconsistent with state-of-the-art Cybersecurity standards (e.g., ISO27001).

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

In this document, the term "business partner" is used throughout to refer to business partners of Siemens and their employees.

The business partner is obliged to adhere to the guidance and regulations of Siemens for the security of IT systems, applications, and networks as set forth herein. Additionally, if requested by Siemens, the business partner shall comply with any other security regulations or guidelines made available to them.

If 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 its 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 engage only personnel qualified in state-of-the-art information security (and secure coding, where applicable) and shall ensure that such personnel refresh and update their training at least once per calendar year.

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

Business partner shall inform Siemens in advance if any personnel assigned to fulfill the contractual obligations are to be replaced. Section 2.6 shall be complied with accordingly.

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"), unless otherwise agreed between the parties.

[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.

Any form used to conceal, distort, or forge the identity or 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 classification level for 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 become 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 classified as “Confidential” shall be stored and processed in encrypted form, and content classified as “Strictly Confidential” shall be encrypted end-to-end.

The business partner shall neither produce copies or reproductions of Content nor delete, examine, or modify such Content without the prior consent of Siemens, 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 requiring user interaction
- e-mails related to critical security services
- e-mails containing potentially 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, and misuse of Siemens e-mail addresses (e.g., adding e-mails to mailing lists without explicit consent) are prohibited, as is the transmission of confidential or strictly confidential Content via fax.

2.2.3. Deletion of Content

The business partner shall reliably delete all Content from all information media that is not, or is no longer, relevant for the provision of the contractually agreed tasks or activities, except where retention is contractually agreed or required under applicable laws and regulations.

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

Where such Content cannot be deleted for legal or physical reasons, business partner shall notify Siemens in writing as to the scope, retention period, and location of said Content and shall implement appropriate security controls to maintain its confidentiality.

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 means of a Siemens provided access solution, depending on the protection level of the respective IT system,

application, and network (e.g., Siemens' business partner access solutions).

If requested by Siemens, business partner shall implement and adhere to Siemens' Zero Trust security framework for any personnel and IT systems used for the provision of the contractual obligations.

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

The business partner shall exercise only those system access and admission authorizations (e.g., passwords or access cards) that have been granted for the fulfillment of its contractually agreed tasks and activities. Such system access and admission authorizations shall be restricted according to the principles of "least privilege", "need to know", and "segregation of duties".

Business partner shall promptly inform Siemens of any changes regarding its employees or subcontractors who have access to Content.

All admissions, related technical configurations, and cryptographic materials shall be kept confidential and shall neither be shared with any third party nor made public.

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

2.4. System and Data Access Protection

IT systems and information media provided by Siemens or used by the business partner to fulfill its contractual obligations must be protected against unauthorized access, including physical security for the business partner's working environment, using 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:

- Using theft protection mechanisms for mobile systems.
- Preventing misuse or unauthorized access when sharing resources.
- Using different passwords per user account (anonymous and guest access shall be disabled).
- No elevation of access privileges without Siemens' prior approval.
- Switching off voice-controlled smart devices or any webcams in the working area that are not required for business purposes (e.g., Amazon Alexa, Apple Siri).
- Logging off and securely storing devices when not in use.
- Ensuring that paper documents containing confidential or strictly confidential Content are not left accessible or unattended; such documents must be locked away using appropriate protection mechanisms.

2.4.2. IT systems and information media owned by business partner

In addition to section 2.4.1, the following minimum protection measures apply to IT systems and information media owned by business partner:

- Installing the current Bios version and activating Bios password protection.
- Prohibiting the use of permanent local administration rights.
- Enabling a password-protected screensaver on the operating systems (i.e., system lock for unattended systems).
- Activating hard-disk and file encryption.
- Ensuring state-of-the-art protection against viruses and other 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 network access via password, at minimum, to protect against illicit and malicious network traffic (e.g., white listing).

- Prohibiting the use of standard passwords; initial passwords must be deleted after receipt and expire after 24 hours.
- Creating passwords from a combination of uppercase and lowercase letters, numerals, and special characters. Passwords must contain at least 12 characters (26 characters for administrator accounts). PINs must use arbitrary numerals. Passwords must be changed every 180 days (45 days for privileged administrative accounts), unless used as part of a two-factor authentication. The last 10 passwords must not be reused. If the business partner is unable to adhere to such password requirements, it must ensure that a state-of-the-art password policy is enforced (e.g., based on Google strong password recommendations or security.org password check).
- Using two-factor authentication for access to confidential and strictly confidential Content.
- Preventing data exchange across network zones (e.g., the Internet) while accessing Siemens IT systems or networks; multiple simultaneous network connections must be avoided.
- Prohibiting the use of network or system analysis devices without Siemens' explicit prior approval.
- Ensuring that network devices connected to, and third-party software used on such devices, are regularly supported and maintained and have current security patches applied.
- If requested by Siemens, installing Siemens-provided intrusion detection appliances and agents for vulnerability management and endpoint detection and response (EDR), and providing Siemens' cyber defense analysts with the Content collected by such appliances and agents.

2.5. Information Obligation, Cybersecurity Contact, Monitoring

2.5.1. Information obligation

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

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

2.5.2. Cybersecurity contact

In addition to notifying the respective Siemens contact persons, the following Siemens Cybersecurity contact addresses shall be informed immediately in the event of any:

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

that potentially or actually results in a breach involving Content, IT systems, applications, networks, or information media.

2.5.3. Monitoring

Siemens monitors and assesses business partner's adherence to these rules and principles as described herein. IT systems connected to Siemens' networks are checked for security vulnerabilities using state-of-the-art methodologies. 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 with the rules and principles set forth herein in a manner consistent with applicable legislation (e.g., retention periods).

If the business partner disregards the rules and principles contained herein, Siemens may disable its access to Siemens sites and IT systems and may enforce the applicable contractual or legal consequences.

2.6. End of Business Relations

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

- Return all IT systems, devices, Content, information media, paper documents, and work equipment (including access cards).
- Return all granted accesses and provide a declaration of such accesses for the purpose of deactivation or deletion (e.g., access to file shares, service accounts, etc.).
- Delete Content on all information media and destroy paper documents in accordance with section 2.2.3.
- Uninstall any software provided by Siemens for fulfillment of the contractual obligations (e.g., virtual client software).