SIEMENS

Be aware, be secure

Information Security

Rules for Business Partners

Date:	2015-09-18
Version:	1.0
Owner:	Siemens Chief Information Security Officer
Published by:	GS IT ISEC

1. Scope and Applicability

The Rules for Business Partners apply to business partners of Siemens who have access to IT systems, applications, networks or company proprietary information[1] of Siemens 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).

1.1. Responsibilities

the business partner of Siemens is granted access to IT systems, applications, networks or company confidential information of Siemens is granted to to fulfill his contractual obligations and to increase the efficiency of business processes.

This requires measures for the protection of IT systems, applications, networks and company confidential information 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.

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 who have access to IT-systems, -applications and networks of Siemens or receive Siemens company properitary information. The business partner shall monitor such compliance in a suitable manner.

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

2. Rules and Principles

2.1. Handling Information

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

Corporate proprietary information of Siemens is all information which is not in the public domain. For corporate proprietary information 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 has to comply with measures that are more stringent as the need for protection increases.

The business partner defines the level of confidentiality of the information 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 information entrusted.

Corporate proprietary information shall only be stored and processed on IT-systems, applications and file storage systems that guarantee an adequate protection of the information.

The business partner is obliged to enable the transmission of encrypted E-Mails (with confidential or strictly confidential content) and the decryption of received encrypted E-Mails.

The automatic forwarding of incoming E-Mail to external mailboxes is prohibited as well as the transmission of confidential or strictly confidential information via fax.

[1] Information of 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).

The business partner shall delete reliably all information of Siemens 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.

Electronic information stored on IT-systems shall be deleted with the standard delete functions during normal operations as long as encryption is enabled. If no encryption has been enabled, the information shall be deleted with an adequate method, comparable to standard DOD 5220.22-M.

Documents in paper format shall either be destroyed with an appropriate document shredder with protection level 6 of EN 15713:2009 or via a shredder service provider. If none of the options are feasible, the business partner shall align its course of action with its contact from Siemens (e.g. usage of Siemens internal facilities).

2.2. System Access and admission authorizations

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. They shall be kept confidential and shall be neither shared with any third party nor made public.

2.3. 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 via state of the art measures. The following measures are minimal protection measures for IT systems information media:

- Bios password.
- Screensaver with password protection of the operating systems (as system lock for unattended IT systems).
- Theft protection for mobile systems.
- 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.
- Securing of network access via password as minimum.
- No unauthorized access when sharing resources.
- Use of different passwords per user account.
- No use of standard passwords. Deletion of initial passwords after receipt.
- Passwords shall be created from a combination of uppercase and lowercase characters, numerals and special characters. Passwords shall contain a minimum of 8 characters (16 characters for administrator accounts). For PINs arbitrary numerals shall be used. Passwords shall be changed every 90 days (30 days for privileged administrative accounts). The last 10 passwords shall not be reused.
- Paper documents containing confidential or strictly confidential information shall not be openly accessible or left unsupervised. They shall be locked away with appropriate protection mechanisms.

2.4. Information Obligation, Monitoring

The defined contact persons by Siemens and the business partner will inform each other 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 and incidents with potential impact on information security, it will notify Siemens immediately, e.g. suspicion of misuse or disclosure of PINs/passwords.

The business partner is obliged to adhere to the guidance and regulations of Siemens for the security of IT systems, applications and networks. A disciplinary authority over the business partner does not exist

Siemens controls and monitors business partners' Adherence to these rules and principles. IT systems connected to

the networks of Siemens are checked for security vulnerabilities according to state of the start methodology. Identified vulnerabilities must be remediated by the business partner without undue delay. All security relevant patches and hotfixes released by the vendors respective must be installed.

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

2.5. End of Business Relations

At the end of business relations with Siemens and unless otherwise agreed, the business partner shall conduct the following activities and confirm in writing:

- Return of all IT systems, devices, information, information media, paper documents and work equipment.
- Return of all granted accesses and declaration of these accesses for the purpose of deactivation or deletion (e.g. access to file shares).
- Deletion of information on all information media and destruction of paper documents in accordance to section 2.1.

2.6. Additional Rules for Business Partners with a Connection to Siemens IT Systems, Applications and Networks

The business partner is obliged to operate the connection only using the technical configuration agreed with Siemens and on the IT systems provided for this purpose.

Information about the structure, accesses (e.g. network addresses) and security measures of the Siemens IT systems, applications and networks are corporate proprietary (see section 2.1) and are to be handled as such by the business partner.