

SGRE IT Cybersecurity

Third Party IT Cybersecurity Requirements

Table of Content

1. PURPOSE.....3

2. SCOPE.....3

3. REQUIREMENTS DESCRIPTION.....3

 3.1. Management direction for IT Cybersecurity 4

 3.2. Human Resource Security 4

 3.3. Asset Management 4

 3.4. Access Control 5

 3.5. Cryptography..... 5

 3.6. Physical and Environmental Security..... 6

 3.7. Operations Security..... 6

 3.8. Backup 6

 3.9. Logging and monitoring..... 6

 3.10. Technical vulnerability management..... 6

 3.11. Communications Security 7

 3.12. System Acquisition, Development and Maintenance..... 7

 3.13. IT Cybersecurity Security Incident Management 8

 3.14. End of Business relations..... 8

 3.15. Compliance 8

 3.16. Liability and indemnity..... 9

4. ABBREVIATIONS AND DEFINITIONS.....9

1. PURPOSE

Third Parties are sometimes granted access to Siemens Gamesa Renewable Energy and affiliated companies' (hereinafter referred to as "SIEMENS GAMESA") Cyber-infrastructure or Corporate Information to fulfill their contractual obligations. This requires measures for the protection of the SIEMENS GAMESA Cyber-infrastructure and SIEMENS GAMESA's Corporate Information to prevent unintentional disclosure, unauthorized access, data loss or manipulation and other cybersecurity threats.

This document describes the minimum IT Cybersecurity requirements the Third Party needs to comply with to work with SIEMENS GAMESA, outlining detailed requirements relevant for Third Parties' own IT systems, applications or networks in case these are used for handling of SIEMENS GAMESA company proprietary information.

In this document, the term "Third Party" is used throughout to refer to third party companies and their employees.

2. SCOPE

The Third-Party IT Cybersecurity requirements apply to all Third Parties who have access to SIEMENS GAMESA's Cyber-infrastructure or Corporate Information due to a contractual relationship. The defined rules and principles herein apply independently whether the Third Party uses IT systems of SIEMENS GAMESA or its own IT systems, if the Third Party works in a SIEMENS GAMESA office or not, or if a connection to IT resources of SIEMENS GAMESA is set up (e.g. to an IT system or an application).

When the Third Party is expressly authorized by SIEMENS GAMESA to subcontract, the Third Party undertakes that the subcontractor shall assume the same obligations assumed by the Third Party under this condition, and in any case, the Third Party shall be liable for any breach by the subcontractor or its personnel of the obligations here established.

3. REQUIREMENTS DESCRIPTION

Data or information, related to the Contract that is property of SIEMENS GAMESA or the Cyber-infrastructure elements provided to the Third Party by SIEMENS GAMESA, shall only be processed and used by the Third Party for the purpose of fulfilling the obligations contained within the Contract and for no other purpose whatsoever.

The Third Party shall, at least, maintain technical and organizational security measures consistent with the type of SIEMENS GAMESA's Corporate Information being processed and the services being provided by the Third Party.

As part of such security measures, the Third Party shall provide a secure environment for all SIEMENS GAMESA's Corporate Information and any hardware and software (including servers, network, and data components) to be used by the Third Party as part of its performance under the Contract.

For that purpose, it is necessary that the Third Party engages and ensures compliance with the following rules and principles and that protective measures are not deactivated, circumvented or changed in any other way.

The Third Party shall comply with the herein defined rules and principles in addition to the contractual agreement. This document must be brought to the attention and consistent adherence to the Third Party's employees who have access to SIEMENS GAMESA's Cyber-infrastructure or Corporate Information. The Third Party shall monitor such adherence in a suitable manner.

Any change to the security requirements described in this document, both from the SIEMENS GAMESA side and the Third Party, must be reviewed and approved by the responsible figures or individuals on both parties before being considered accepted.

3.1. Management direction for IT Cybersecurity

The Third Party must have defined an IT Cybersecurity / Information Security Policy Framework, which shall have been approved by management, published and communicated to employees and relevant external parties.

The Third Party must ensure that the rules specified in the IT Cybersecurity / Information Security Policy Framework and in any other cybersecurity or information security regulation are complied with by all units and affiliated companies of the Third Party and reviewed regularly and after major changes in the organization.

3.2. Human Resource Security

In order to fulfil the purpose of the Contract, SIEMENS GAMESA may make available to the Third Party's Personnel or its subcontractors or subsidiaries any data, electronic devices or other computerized media or resources. For the same purpose, SIEMENS GAMESA may provide a SIEMENS GAMESA email account or credentials for accessing applications, internet connectivity, or other Cyber-infrastructure elements of SIEMENS GAMESA. In case any of these situations are true, the Third Party shall be responsible for ensuring that its Personnel and subcontractors are informed and expressly commit to comply with the security and acceptable use conditions established by SIEMENS GAMESA, which shall be provided in a separate appendix (IT Acceptable Use Policy).

The Third Party shall retain the evidence that prove compliance with these duties and shall deliver them to SIEMENS GAMESA upon request.

3.3. Asset Management

The Third Party shall ensure that IT assets, information data and single documents are classified according to their business value and potential risk impact and shall adopt the technical and organizational security measures adequate thereto. The classification level assigned to documents and ownership shall be labeled clearly and easily visible regardless of whether the document is on paper or electronic form.

SIEMENS GAMESA's Corporate Information shall only be stored and processed on IT Assets which comply with all applicable cybersecurity or information security regulations, including the requirements specified in this document.

The Third Party must ensure that SIEMENS GAMESA's electronic Corporate Information is stored encrypted and shall establish adequate procedures to guarantee protection against loss or unauthorised access.

Data storage media containing SIEMENS GAMESA's Corporate Information shall be either physically destroyed or the data shall be irretrievably erased at the end of the storage media lifecycle, prior to reuse of the storage media, or when the information is no longer required. SIEMENS GAMESA's Corporate Information in paper form shall be destroyed to prevent reconstruction in whole or in part.

The Third Party shall avoid storing any SIEMENS GAMESA's Corporate Information on portable equipment or mobile devices. In case they are used, the Third Party must ensure that these IT Assets guarantee the same protection against loss or unauthorised access to SIEMENS GAMESA's Corporate Information as non-portable devices.

The Third Party shall implement a procedure for lost or stolen equipment or devices which ensures the prompt notification to SIEMENS GAMESA, the safe remote wipe out of the device in accordance with recognised standards and the suspension of access to SIEMENS GAMESA's systems to the affected user.

3.4. Access Control

The Third Party shall establish the mechanisms and procedures for identifying, authenticating and controlling logical access necessary to prevent unauthorized personnel from accessing its Cyber-infrastructure elements and SIEMENS GAMESA's Corporate Information.

The Third Party shall define access control procedures based on the principle of least privilege when granting, assigning and withdrawing authorized access and permissions to Personnel of the Third Party or its subcontractors, including privileged users or administration.

The Third Party shall define policies and procedures that ensure the strength of the access credentials (e.g. passwords) and that they are updated regularly, including:

- Access to IT systems and applications that store SIEMENS GAMESA's Corporate Information must require, at least, single-factor authentication and strong authentication (e.g. Multi Factor Authentication) must be enforced when data criticality and risk exposure is significant based on the Third Party's risk management process. The Third Party must ensure that IT systems and applications force password length and password complexity requirements following state-of-the-art best practices and force the change of passwords periodically when used as single-factor authentication.

The Third Party must ensure at least the following requirements regarding user access management:

- User accounts are only assigned to and used by single persons.
- Service accounts and shared user accounts shall have a person assigned who holds the overall accountability for the account and ensures that the accounts are properly used.
- Unique identifiers (IDs) shall be assigned to accounts on IT systems and applications.
- Privileged access rights to IT systems, applications, and network services shall only be granted to individuals who need it to accomplish their tasks.

The Third Party must maintain an updated inventory of the access and permissions granted to SIEMENS GAMESA's Cyber-infrastructure. The Third Party will inform SIEMENS GAMESA of its Personnel who cease working and have access to SIEMENS GAMESA's Cyber-infrastructure on the shortest period of time possible and withdraw access permissions promptly.

The Third Party must ensure that the users are aware of, at least, the following responsibilities regarding their passwords:

- For each account a different password shall be used.
- Passwords shall not be trivial or easy to guess and shall be created following the requirements for complexity and length recommended by state-of-the-art best practices.
- PINs and passwords shall be changed immediately, or its change forced at next logon if there is suspicion of misuse or disclosure.
- Personal secret authentication information shall not be shared with others.
- Old passwords shall not be reused.

The Third Party must ensure that secret authentication information, including their hashed values, is transmitted encrypted.

3.5. Cryptography

The Third Party must ensure that only secure and strong cryptographic material is used based on state-of-the-art best practices. Vulnerable encryption algorithms or protocols are not allowed.

3.6. Physical and Environmental Security

The Third Party must ensure that SIEMENS GAMESA's Corporate Information is stored or processed only in areas which are adequately protected with physical measures based on a risk, threat, and vulnerability analysis so as to prevent unauthorised personnel from accessing it during the time in which the Third Party has access to SIEMENS GAMESA's Corporate Information.

The Third Party must ensure that IT areas and data centers are protected with adequate security physical measures based on the classification level of the information hosted and processed.

Before reusing or disposing an IT system, the Third Party must ensure that the data on its data storage media has been irretrievably erased or the data storage media has been physically destroyed.

3.7. Operations Security

The Third Party must define standards and baselines for the secure configuration of IT systems and applications, based on state-of-the-art best market practices and vendor recommendations, and ensure all IT systems and applications that process SIEMENS GAMESA's Corporate Information or access SIEMENS GAMESA's Cyber-infrastructure are configured following these.

The Third Party must ensure that IT systems and applications in non-production environments fulfill the same IT Cybersecurity requirements as IT systems and applications in production environments if they host or process productive data.

The Third Party shall ensure that IT systems that process SIEMENS GAMESA's Corporate Information or access SIEMENS GAMESA's Cyber-infrastructure are protected against malicious software by implementing appropriate and state-of-the-art anti-malware solutions.

3.8. Backup

The Third Party shall implement the technical and organisational measures necessary to ensure operational continuity under the service level agreements adopted for the Contract (including but not limited to contingency plans, backup and recovery procedures).

The Third Party must ensure that a backup concept for IT systems and applications that process SIEMENS GAMESA's Corporate Information, which includes data and configuration settings, is defined, documented, and implemented. The backup concept shall make backup copies of SIEMENS GAMESA's Corporate Information as frequently as required for the performance of the Contract and according to the nature of the data, establishing the appropriate procedures and mechanisms to ensure that the data can be retrieved. The same security measures shall apply to backups as to the original SIEMENS GAMESA's Corporate Information.

The Third Party must determine, document and guarantee the availability requirements of IT systems and applications that support SIEMENS GAMESA's information and business processes.

3.9. Logging and monitoring

The Third Party must ensure that security-relevant events on IT systems and applications are defined and logged.

3.10. Technical vulnerability management

The Third Party must check IT systems and applications for security vulnerabilities on a regular basis.

The Third Party must ensure that technical vulnerabilities on IT systems and applications are mitigated, and that vendor security fixes and updates are implemented on the applicable IT systems and applications. The mitigations period must be established based on the vulnerability criticality, and the exposure and criticality of the associated IT system and applications to assure the vulnerabilities are not exploited.

The Third Party must ensure that IT systems or applications versions no longer supported by the vendor or whose development has been discontinued are not used and are removed from IT systems.

3.11. Communications Security

The connection between SIEMENS GAMESA's and the Third Party's network is not permitted, unless expressly agreed to in the Contract, in which case it must be done by following the technical configuration defined by SIEMENS GAMESA.

The Third Party must ensure that all SIEMENS GAMESA's electronic Corporate Information is transmitted encrypted.

The Third Party is not authorised to disclose, provide direct or indirect access to SIEMENS GAMESA's Corporate Information or provide it to other Third Parties or subcontractors, including affiliates, even for storage purposes, unless expressly agreed to in the Contract.

The connection with the Third Party's network shall be removed as soon as there is no need for it.

3.12. System Acquisition, Development and Maintenance

The Third Party must ensure that IT Cybersecurity requirements are identified and documented prior to the development and acquisition of new IT systems and applications as well as before improvements to existing IT systems and applications are made.

The Third Party shall include security measures appropriate to the nature of the information processed in developing, maintaining and testing the equipment that will be used in fulfilling the Contract. The Third Party will adopt secure code development standards and ensure that no real data is used in test environments. If necessary, SIEMENS GAMESA's express authorisation will be required and the same security measures required for the work environment will be applied to these test environments.

When the scope of the Contract includes the supply of equipment and/or materials, the Third Party shall prove that best security practices and standards have been applied for the design, fabrication, maintenance, and, where applicable, installation of the supplied equipment and/or materials, including its components.

For any such equipment and/or materials with information processing capacity or network connectivity options:

- The Third Party shall provide evidence or certificates that guarantee design security, firmware/software updates and malware protection.
- The Third Party shall conduct periodic analyses of vulnerabilities and inform SIEMENS GAMESA about any necessary updates, especially those that affect security.
- All internet connected devices shall be protected with non-trivial passwords that have been created following the requirements for complexity and length.
- The configuration of devices, equipment and materials shall be adjustable exclusively according to SIEMENS GAMESA's needs, and any unnecessary functionality deactivated. Should the Third Party conduct any configuration, documentation to that effect shall be provided.

3.13. IT Cybersecurity Security Incident Management

The Third Party shall implement a procedure to notify of and manage any data breach or IT Cybersecurity incidents, which it will disclose among its Personnel, and will act with special diligence in those cases involving critical elements of SIEMENS GAMESA's Cyber-infrastructure or Corporate Information or when the reputation or legal responsibility of SIEMENS GAMESA or the interests of the persons whose information is processed may be affected.

The Third Party shall immediately notify SIEMENS GAMESA of the existence of any security incident, information security weaknesses or deficiencies on IT systems and applications always as soon as detected and always ensuring compliance with the shortest legal period requested by the applicable regulations, and shall assist and cooperate with SIEMENS GAMESA in terms of any necessary communication to third parties and other reasonable measures to remedy the situation when SIEMENS GAMESA requests it or as required by law.

3.14. End of Business relations

Once the Third Party's contractual performance has been completed, or in the event of a termination of the Contract, the Third Party shall return to SIEMENS GAMESA or securely destroy, at SIEMENS GAMESA's choice, all information owned by SIEMENS GAMESA that may be in its possession, as well as any media or document that includes SIEMENS GAMESA's Corporate Information. Should information destruction be selected, the Third Party shall provide its corresponding certification by following recognised standards for doing so.

Furthermore, all equipment, devices and storage media owned by SIEMENS GAMESA shall be returned and any potential connectivity to SIEMENS GAMESA's Cyber-infrastructure will be suspended. The same shall occur whenever the infrastructure elements or information are no longer needed for the performance of the Third Party's obligations under the Contract.

If the Third Party is required by applicable law to retain SIEMENS GAMESA's Corporate Information, it shall keep both the information and the items that contain it duly protected and only for the time necessary in accordance with applicable laws and regulations. Once said period has lapsed, they will be destroyed or returned to SIEMENS GAMESA, at SIEMENS GAMESA's choice, as will any media or documents containing any such data and no copy of the information will be kept.

3.15. Compliance

The Third Party shall ensure compliance with all applicable data protection, privacy and security laws and regulations and shall not place SIEMENS GAMESA, by act or omission, in a situation of non-compliance.

The Third Party shall ensure that the equipment that will be used in fulfilling the Contract complies with all applicable intellectual property rights, software licenses requirements, and regulations.

At SIEMENS GAMESA's request, the Third Party shall provide evidence of security assessments or audits. SIEMENS GAMESA shall have the right to conduct independent audits and/or inspections of the Third Party's security measures at its data processing facilities and any cloud storage services. Such audits or inspections shall be conducted by SIEMENS GAMESA or by a representative or audit agency approved by SIEMENS GAMESA. The Third Party undertakes to comply with the possible plan of action that may result from said audits. The Third Party shall ensure the implementation of the action plan that may result from said audits.

The Third Party shall provide SIEMENS GAMESA with reasonable and timely support in responding to any request, complaint or other communications received by any individual, government, governmental agency, regulatory authority or other bodies that may have an interest in the use, leakage, disclosure

or misuse of any data or information related to the Contract, insofar as they comply with processing the data or information by the Third Party.

SIEMENS GAMESA must be informed in advance of any communication of SIEMENS GAMESA data that the Third Party must perform pursuant to a legal or judicial provision.

3.16. Liability and indemnity

The Third Party shall be liable for any non-compliance of the obligations set forth in this document by any of its shareholders, administrators, Personnel, assignees, subcontractors or professional advisers (hereinafter, its "Representatives") who have had access to SIEMENS GAMESA's Corporate Information. SIEMENS GAMESA reserves the right to take pertinent legal actions to defend its interests regarding the non-compliance.

The Third Party will indemnify SIEMENS GAMESA for all losses, claims damages, expenses and costs suffered or incurred by SIEMENS GAMESA directly or indirectly from the non-compliance by the Third Party and/or by any of its Representatives of the obligations provided for in this document or the disclosure or unauthorised use of the SIEMENS GAMESA's Corporate Information.

4. ABBREVIATIONS AND DEFINITIONS

Abbreviation	Description
SGRE	Siemens Gamesa Renewable Energy

Definitions	Description
Cyber-infrastructure	Electronic information and communication systems and services, as well as the information contained therein. These systems can be both housed within the facilities as well as cloud-based and can be proprietary or third-party owned. The systems are comprised of hardware and software for processing (creating, accessing, modifying and destroying), storing (on magnetic, electronic or other formats) and sending (shared use and distribution) information, or any combination of said elements. These systems can include any type of electronic device such as, without limitation, standard computers (desktop/laptop) with internet connections, digital storage methods used on computers (e.g. hard drives), mobiles, smartphones, personal digital assistants, data storage media, digital and video cameras (including CCTV), GPS systems, IoT devices, etc.
Corporate Information	Any information created, received, transmitted or stored that by its nature or value to SIEMENS GAMESA requires reinforced protection measures, including but not limited to Confidential Information, Company Data, private or secret information, personal data, credit card data, commercially sensitive information, critical infrastructure information, strategic business information, credentials, encryption data, system and application access logs, or any other information that may be affected by a regulation or may impact SIEMENS GAMESA.