

SGRE IT Cybersecurity IT Acceptable Use policy



Table of Content

1. PURPOSE.....3

2. SCOPE.....3

3. POLICY DESCRIPTION3

 3.1. General Use and Ownership..... 3

 3.2. IT devices 3

 3.2.1 External data storage and removable devices..... 4

 3.2.2 Out of the office 4

 3.2.3 Use of personal IT devices..... 4

 3.3 Software 5

 3.3.1 Credentials 5

 3.4 Communications 6

 3.4.1 Internet 6

 3.4.2 Email 6

 3.4.3 Telephone 7

 3.4.4 Remote Access 7

 3.5 Information and data handling 7

 3.6 Incident handling 8

 3.7 Logging, monitoring and supervision 8

4. ABBREVIATIONS AND DEFINITIONS.....9

1. PURPOSE

The purpose of this policy is to establish rules for acceptable and unacceptable use of IT devices, software and communication resources at Siemens Gamesa Renewable Energy and affiliated companies (hereinafter referred to as “**SGRE**”) in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.

These rules are in place to protect the user and SGRE. Inappropriate use exposes SGRE to risks including malware attacks, compromise of network, systems and services, and legal issues.

This policy must be read in conjunction with the applicable laws (including, without limitation, data protection laws, labor laws, etc.), local policies and employers/works council agreements.

2. SCOPE

This policy applies to all SGRE personnel with any type of employment contract, including e.g. interns, temporary workers from employment agencies, as well as any other person who uses SGRE's IT assets due to his/her professional, business or technological relationship with SGRE (hereinafter referred to as “**User/s**”).

3. POLICY DESCRIPTION

SGRE provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives of SGRE and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets.

SGRE's regulation and control of the User's use of the IT devices, software and communication resources according to this policy will always be carried out with due respect for existing laws, collective agreements and employers/works council agreements.

All User oriented procedures and standards referenced in this document can be found in Explore IT Portal's Knowledge Base.

3.1. General Use and Ownership

The IT devices, software and communication resources (hereinafter referred to as IT assets) that SGRE makes available to the User shall at all times be the property of SGRE.

SGRE's proprietary information stored on IT assets remains the sole property of SGRE, no matter whether the IT asset is owned or leased by SGRE, the User or a third party.

IT assets must be protected from improper use, including, among others, theft, unauthorized access, fraudulent manipulation and alteration of data, attempts to bypass security controls and any activity that could compromise the IT assets.

The User has responsibility to promptly report the theft, loss or unauthorized disclosure of the SGRE's proprietary information and/or IT assets.

The User may access, use or share SGRE's proprietary information only to the extent it is authorized and necessary to fulfill the assigned job duties.

Users are responsible for making proper and safe use of any IT asset of SGRE. The appropriate use includes the use of IT infrastructure in a responsible and professional manner, including exercising good judgment regarding the reasonableness of personal use.

The public reputation of SGRE plays an important role for its credibility and image. Thus, the internet access, email account and other electronic media placed at the User's disposal in connection with the carrying out of his/her work may not be used in a way which is either illegal or may affect SGRE's reputation.

3.2. IT devices

The IT devices supplied by SGRE constitute a corporate service made available to the User and its use is restricted to legitimate business purposes. Personal use is permitted where such use is reasonable, proportional and in accordance with the contractual obligation of good faith, it does not affect the User's business performance, is not detrimental to SGRE in any way, not in breach of any term and condition of employment and does not place the User or SGRE in breach of statutory or other legal obligations.

All IT devices are subject to the standardizations and approvals established by SGRE and they cannot be modified and/or upgraded by the User without SGRE's prior consent.

It is forbidden to use IT devices (PC's, printers, etc.) connected directly to the SGRE corporate network, or to elements which are connected to the SGRE corporate network and which have not been previously approved by SGRE. If the use of any non-approved hardware is detected, SGRE could deny giving support to it, demand to stop using it or disconnect it from the network.

IT devices must be protected when they are not being attended or are not being used. The session must be locked or logged off when the device is unattended, and access must be controlled by a password, token or combination of User authentication mechanisms. The computers must be switched off or hibernated when there are absences in the workplace.

At the end of each day and regardless of where the User may be, portable IT devices shall be kept under lock and key or, lacking that, in a secure place, so as to avoid any risk of theft or loss.

Users must return to SGRE all IT devices that have been assigned to them, or that are in their possession, at the time or prior to the date of termination of the contract, when it is determined that their use is not necessary anymore or upon SGRE's request. It is the user's responsibility to remove all the personal information which might have been stored in the IT devices before they are returned to SGRE, which is entitled to fully dispose of the IT devices and their content as per clause 3.7.

3.2.1 External data storage and removable devices

It is not permitted to use personal removable devices (e.g. USB storage devices) to make back-ups or share SGRE's information.

The use of external data storage devices is restricted to those cases in which the storage and/or sharing of information cannot be carried out by the common means made available by SGRE (e.g. OneDrive, Sharepoint). Only SGRE approved removable devices with standardized security measures in place (e.g. encryption) are allowed for those cases.

3.2.2 Out of the office

IT devices must be only used in secure places and never be left unattended.

The User must watch the IT device when in public places such as airports, cafes, restaurants and also while at customer's or vendor's offices. In these situations, the User must not leave the computer unattended/unsecured at any time.

The use of IT devices in public places that could expose proprietary information to espionage, eavesdropping or general unauthorized access must be avoided. The use of privacy screen protectors is highly recommended.

3.2.3 Use of personal IT devices

The purpose of this section is to define accepted practices, responsibilities and procedures for the use of personally owned IT devices (such as smartphones and tablets) that SGRE authorizes to connect to corporate systems. This section defines the commitment requirement, provides guidance for the secure use of personal IT devices and the data contained on those devices.

The access to enterprise systems using personal IT devices is an opt-in decision.

In instances where personal IT devices are permitted for business use, the User must ensure that the mobile apps used for accessing SGRE corporate data and the data contained in them are compliant with all sections of this policy.

Users must agree to keep up to date and in good working order all personal IT devices and platforms used for accessing enterprise systems.

Users must maintain a device compatible with the organization's technical specifications. If a device falls out of compliance, then it may be blocked from access until it is in good working order and meets minimum requirements.

The device functionality must not be modified unless required or recommended by SGRE. The use of devices that are jailbroken, "rooted" or have been subjected to any other method of altering or disabling built-in protections is not permitted.

Users must allow the installation of an enterprise procured IT device management software agent, or any other software deemed necessary, on the user's personal IT device subject of this policy, in order to access SGRE IT assets on their personally owned device.

Users must accept that, when connecting a personal IT device to SGRE resources, the SGRE's security policy will be enforced on the device. The security policy implemented may include, but is not limited to, policy elements such as passcode, passcode timeout, passcode complexity and encryption.

The scope of the installed IT device management software agent is limited to the corporate applications and data contained wherein. The security policies will only be enforced to the corporate applications that are managed by the IT device management software agent. The personal applications and data that are not used to access SGRE corporate infrastructure and information will not be enforced to comply with these policies.

The User is responsible for notifying SGRE prior to replacing or sending their personal IT device to a third party (e.g. for repair), as well as when the personal IT device is lost, stolen, retired or otherwise compromised. Users must accept that SGRE has the right to wipe the corporate data that is stored in the personal IT device in these cases, or when a User is separated from SGRE through resignation, termination or layoff.

Users are responsible for upgrades, including backing up and restoring data as part of the upgrade process. Users are solely responsible for backing up any personal content on the device.

Users must use SGRE sanctioned network file shares (e.g. Office 365) for the purpose of synchronizing organization information between IT devices, and may not for that purpose use unapproved, cloud-based personal file synchronization services (e.g. Google Drive, Dropbox, iCloud, etc.).

Users must take appropriate precautions to prevent others from obtaining access to the personal IT devices.

3.3 Software

The installation of software not approved by SGRE on laptops, PCs and servers owned by SGRE is forbidden. The acquisition and installation of new software in these platforms must be requested through IT established procedures (e.g. Explore IT Portal).

The installation of mobile apps via Apple Store (iOS) and Play Store (Android) in smartphones and tablets owned by SGRE is generally accepted, except for mobile apps that have been blacklisted by SGRE. A list of blacklisted mobile apps can be consulted in the Explore IT Portal's Knowledge Base.

The software supplied by SGRE or the documentation accompanying it shall not be copied for personal purposes. The licensing agreements do not cover the software's domestic use.

The installation of any type of peer-to-peer network (P2P) or similar network access program (e.g. BitTorrent, Emule), as well as any other application for the exchange of files that saturates the bandwidth of the network, preventing access to other Users or slowing down connections to the technological and IT resources of SGRE is strictly prohibited.

Intellectual property, licenses and any other laws and regulations in this respect must be respected at all times. It is forbidden to download, obtain, copy or redistribute material subject to copyright (including software, music, video and images) if this violates any law or regulation of any jurisdiction, even if the material is used for performance of a professional activity.

The use of any software or services on SGRE owned devices and IT infrastructure that do not have the relevant licenses for use or, in general, whose use is contrary to any regulation is prohibited.

In those cases in which material subject to copyright is required to carry out a professional activity, the corresponding license must be obtained through the established formal channels.

3.3.1 Credentials

Passwords, Usernames and any other kind of credentials used to identify individuals as a User of the SGRE's IT assets and that allow access to them should not be passed on to other people or shared under any circumstances, including requests that come from management or computer support services, nor should they be written down where they can be seen by other people.

The User must guarantee the credentials' confidentiality to protect the information contained in the assigned equipment and safeguard the intellectual property of SGRE. The use of a password management software provided by SGRE is encouraged (e.g. KeePass).

Passwords shall be created following the requirements for complexity and length required by SGRE in the specific security standard.

Users must modify the secret authentication information whenever there is any indication that it has been compromised. Any incident or indication that said authentication information is being compromised must be reported by following incident notification procedures.

3.4 Communications

Connection to networks is a corporate service that SGRE places at the Users' disposal and its use is restricted to legitimate business purposes.

Users should under no circumstances alter the configuration parameters of their communications resources, nor allow others to do so. Any connection problems should be diagnosed and dealt with according to IT's instructions, and any non-authorized alteration to the network's configuration could be subject to an investigation.

3.4.1 Internet

The use of the Internet is restricted to legitimate business purposes. Personal use is permitted where such use is reasonable, proportional and in accordance with the contractual obligation of good faith, it does not affect the User's business performance, is not detrimental to SGRE in any way, not in breach of any term and condition of employment and does not place the User or SGRE in breach of statutory or other legal obligations.

All Users are responsible for the network activity done under their name and must assume the consequences arising from their performance in case of illegal activities.

Under no circumstances shall visits to websites whose contents appear below be permitted:

- Contents that are defamatory, threatening, offensive or denigrating to people, organizations or groups of any kind.
- Illegal contents or contents geared towards committing illegal actions.
- Content that could put in danger the security of SGRE IT assets or corporate data.
- Content that could suppose a non compliance with this policy (e.g. unauthorized software download).

Likewise, saving any of the materials set forth in this point in the SGRE owned IT devices is strictly forbidden.

As the streaming of music and movies affects the network, streaming should primarily be used for work-related purposes and, furthermore, only to a very limited extent.

SGRE reserves the right to control or limit the set of Internet services accessible to Users for reasons of security or the service's performance, as per clause 3.7.

3.4.2 Email

The email service is a corporate service that SGRE places at the Users' disposal and its use is restricted to legitimate business purposes.

Personal use is permitted where such use is reasonable, proportional and in accordance with the contractual obligation of good faith, it does not affect the User's business performance, is not detrimental to SGRE in any way, not in breach of any term and condition of employment and does not place the User or SGRE in breach of statutory or other legal obligations. The User should classify these emails as "Personal".

All the information created, sent or received through SGRE's corporate email system, including all messages and electronic files, are property of SGRE.

The use of email accounts not provided by SGRE for the performance of professional functions or on behalf of SGRE is prohibited.

Use of resources

Any messages sent by Users should aim to minimize the use of resources. This implies minimizing in so far as is possible the use of attached files and using the tools made available by SGRE for information sharing (e.g. SharePoint or OneDrive).

SGRE reserves the right to establish a size limit for any individual messages processed, and the delivery or reception of any mail exceeding this limit may be cancelled.

Users shall attempt to avoid storing an excessive number of emails, especially those that have extensive attached documents. In order to avoid overloading the computer system in charge of the email service, SGRE reserves the right of setting available space limits for each mail account and the sending and/or reception of messages may be automatically restricted should the limit be exceeded.

Responsible use

Users must make responsible use of SGRE's corporate email, avoiding oversights or inaccuracies that may be misinterpreted.

- All emails shall be classified using the information classification tools made available by SGRE for this purpose. As a standard, the "Restricted" classification level is preselected.
- Emails containing corporate proprietary information must not be automatically forwarded to external email addresses or bulk downloaded and stored locally (PST files).
- It is forbidden to use SGRE's email address to access social networks and similar services that are not directly related to the User's business duty or contracted service.
- It is forbidden to falsify, distort, hide, suppress or replace the identity of a User in any electronic communication system of SGRE to deceive the recipient about the identity of the issuer.

In general terms, any contents contrary to the ethical principles commonly accepted by society, against public order or that breach the fundamental rights of individuals and, more specifically, violent, racist, sexist or pornographic contents shall be avoided.

3.4.3 Telephone

Fixed line telephones, mobile phones and other equipment which may be used for telephony are corporate services that SGRE places at the Users' disposal and their use is restricted to legitimate business purposes. Personal use is permitted where such use is reasonable, proportional and in accordance with the contractual obligation of good faith, it does not affect the User's business performance, is not detrimental to SGRE in any way, not in breach of any term and condition of employment and does not place the User or SGRE in breach of statutory or other legal obligations.

To the extent that the equipment gives access to the internet or emails, the use hereof is regulated by the above-mentioned guidelines.

3.4.4 Remote Access

The remote connection to SGRE 's IT infrastructure must be done using secure channels previously approved by SGRE.

Remote access authorization must be requested through the person responsible for the service at SGRE and must be restricted to the computer resources and / or applications that are required in the context of the User's business duty or contracted service.

Users authorized to connect remotely are prohibited from initiating simultaneous connections to different networks.

Remote desktop connections are not allowed, except those that have been expressly approved by SGRE.

3.5 Information and data handling

Any information / data that is provided to Users for the fulfillment of their professional activities are assets owned by SGRE and the personal data they contain shall be processed in compliance with SGRE's internal policies.

Any information or data obtained or created by the Users during the contractual relationship with SGRE is the property of SGRE and, therefore, should not be retained, re-sent, shared or eliminated without having prior and formal approval of it.

It is every User's duty to classify the information that she or he creates. The author of information is responsible for its classification - according to its business value and potential risk impact for SGRE. The recipient of the information is then bound to this classification and must treat it accordingly.

Corporate information is classified in classes and each class has its own protection requirements. The author of information is obliged to perform the classification, and to display the classification preferably on each page. The document or information shall be labeled in an area where it is easy to read - or if labeling is obviously not possible (e.g. data records in IT systems) the classification shall be communicated by the owner of the IT system. Additional information on the classification of information can be found in POL-46499 IT Cybersecurity Policy.

SGRE's data shall not be stored in any IT device not belonging to or approved by SGRE, regardless if this device is on the network or not. The use of applications or services not approved by SGRE for the sharing or storing of corporate proprietary information (e.g. Dropbox, Gmail) is forbidden.

Any information owned by third parties to which any User may access must be duly respected and the User shall refrain from its use or disclosure without the prior formal authorization of its owner.

Notwithstanding that the User is to a limited extent entitled to store personal documents and files on the SGRE's equipment, this is not recommended as SGRE is at any time entitled to reset the equipment or otherwise delete content kept in the electronic equipment. Any storing of personal documents and files is made entirely at the Users' own responsibility. Thus, the User cannot hold SGRE responsible for changes, damage or miscarriage of any such documents or files.

All SGRE data or intellectual property developed or gained during the period of employment remains the property of SGRE and must not be retained beyond termination of contract or labor relationship or reused for any other purpose.

3.6 Incident handling

An "operating incident" is defined as any situation that could place the confidentiality, integrity or availability of the data contained in any of SGRE's IT assets at risk, such as:

- Malware alerts.
- Improper logical access (e.g. knowledge or suspicion of a User's ID and password being used).
- Improper physical access (e.g. theft, robbery or loss of a User's IT device).
- Incidents related to data protection (e.g. modification of data or files without the User's knowledge).

Users must immediately report to SGRE any operating incident, as soon as the User is aware of its existence, following the applicable incident notification procedures. Should the circumstances require it, SGRE shall commence a confidential investigation on the incident.

3.7 Logging, monitoring and supervision

SGRE reserves the right of setting up the controls it may deem suitable to reinforce and guarantee compliance with the requirements contained in this policy, and to register and / or monitor the IT assets of Users in accordance with applicable laws (including, without limitation, data protection laws, labor laws, etc.), local policies and employers/works council agreements.

SGRE will at any time ensure that control measures must comply with the following principles:

- **Purpose limitation:** They must be (1) objectively substantiated in operational reasons, (2) shall be collected for specific, explicit and legitimate purposes only, and (3) shall not be further processed in a manner that is incompatible with those purposes;
- **Data minimization:** They must be adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed;
- **Reasonableness:** They must neither be offensive to the users nor cause them a loss or noticeable inconveniences, and must be constructed in such a way that they hold a fair proportion between means and measures; and
- **Transparency:** The User must be informed accordingly in an easy-to-understand language.

SGRE will observe these guidelines when exercising control and will only carry out control within the scope of the objectives and limitations stipulated in this policy.

SGRE reserves the right to log all activities on SGRE's IT assets. The logging is done for the sake of IT operations and security as logging can make it easier to find the reason for errors or operational

irregularities. The data collected is limited to that required for the execution of these purposes (e.g. IP address, web address, user names, device identifiers, browser type, etc.).

SGRE reserves the right to access, open and, to the necessary extent, read the information in the IT assets of the User in order to:

1. support the legal and compliance investigations processes (for instance, if there is a specific suspicion of violations of the law or SGRE's internal regulations, e.g. violation of Business Conduct Guidelines, suspicion that business secrets are being passed on);
2. guarantee the security of SGRE's information and IT assets and systems (for instance, in case there is a cyber security or general security violation taking place (or suspected to take place) -e.g. harmful software (malware)-).

If required by SGRE for the investigation of these topics, the User must provide SGRE with all IT devices SGRE has put at the Users' disposal, together with the necessary access codes. This does not prevent SGRE from acting as provided in this clause.

After the User's resignation, SGRE reserves the right to open, read, forward and delete all information in the IT assets of the User to support the continuity of the business operations.

In all cases, it will happen in accordance with the agreed Compliance procedures and in observance of applicable laws (including, without limitation, data protection laws, labor laws, etc.), local policies and employers/works council agreements and the duty of confidentiality will be met at all times.

4. ABBREVIATIONS AND DEFINITIONS

Abbreviation	Description
SGRE	Siemens Gamesa Renewable Energy

Definitions	Description
Communication resource	Any machine, equipment, network or tool capable of serving as an instrument to send or receive electronic communications such as, for instance, the e-mail and Internet services that SGRE places at Users' disposal. Likewise, every messages' data (text, header and traces) residing in the machines SGRE places at the Users' disposal is considered as communication resources.
Explore IT portal	Explore IT portal is the one single source of truth for anything IT in SGRE. It's the self-service portal designed to become the central hub for all IT information and needs for the user. • The "Request something" section helps the User browsing through the catalog for IT services and products and raise requests related to any of them. • The "Knowledge Base" section is a collection of user guides, video tutorials, tips & tricks, and IT announcements and news. • The "Report an Issue" section helps the User contact IT to report an issue and get support.
IT device	The standard computer (desktop / laptop) with network connections, digital storage media used in computers (e.g. hard drives), mobile phones, smartphones, tablets, storage media, digital and video cameras (including CCTV), mobile navigation systems, etc.
User	SGRE personnel with an employment contract, interns, temporary workers from employment agencies, as well as any other person who uses SGRE's IT assets due to his/her professional, business or technological relationship with SGRE.

