

1. Anwendungsbereich

Diese Regelungen für Geschäftspartner gelten für Geschäftspartner von Siemens Energy, die im Rahmen eines Vertragsverhältnisses Zugang oder Zugriff auf IT-Systeme, -Applikationen, -Netze oder Informationen¹ haben.

Die hierin definierten Regeln und Grundsätze gelten unabhängig davon, ob der Geschäftspartner IT-Systeme von Siemens Energy oder eigene IT-Systeme nutzt, der Geschäftspartner in Räumlichkeiten von Siemens Energy arbeitet oder nicht, oder ein Anschluss zu IT-Ressourcen von Siemens Energy erfolgt (z.B. zu einem IT-System oder einer IT-Applikation).

Die Cybersecurity Klauseln einer zugrunde liegenden Vereinbarung bleiben hiervon unberührt.

1.1. Verantwortlichkeiten

Der Geschäftspartner von Siemens Energy erhält Zugang zu IT-Systemen, Anwendungen, Netzwerken oder Informationen, um seinen vertraglichen Verpflichtungen nachzukommen und die Effizienz der Geschäftsabwicklung zu steigern.

Dies erfordert Maßnahmen zum Schutz von IT-Systemen, Anwendungen, Netzwerken und Informationen, um unbeabsichtigte Offenlegung, unbefugten Zugriff, Manipulation, Computerviren, Hacking, Cyberangriffe und andere IT-Sicherheitsbedrohungen zu verhindern. Zu diesem Zweck ist es erforderlich, dass die Geschäftspartner von Siemens Energy die folgenden Regeln und Grundsätze einhalten und dass Schutzmaßnahmen nicht auf andere Weise deaktiviert, umgangen oder geändert werden. Alle diese Maßnahmen sind in Übereinstimmung mit Cybersecurity Standards (z.B. ISO27001) nach dem Stand der Technik durchzuführen.

Der Geschäftspartner verpflichtet sich zusätzlich zu den sonstigen vertraglichen Vereinbarungen, die hierin definierten Regeln und Grundsätze zu beachten sowie diese Unterlage seinen Mitarbeitern und allen Subunternehmern, die Zugang oder Zugriff auf IT-Systeme, -Applikationen und -Netze von Siemens Energy oder Informationen erhalten, zur Kenntnis zu bringen, sie auf die Einhaltung zu verpflichten und die Einhaltung in geeigneter Weise zu überprüfen.

Im Weiteren werden Geschäftspartner und seine Mitarbeiter zusammenfassend als Geschäftspartner bezeichnet.

Der Geschäftspartner ist verpflichtet, die Richtlinien und Vorschriften von Siemens Energy für die Sicherheit von IT-Systemen, Anwendungen und Netzwerken einzuhalten.

Erfüllen Geschäftspartner ihre vertraglichen Verpflichtungen aus der Ferne/Remote (weder bei Siemens Energy noch auf Geschäftspartnergelände), so hat der Geschäftspartner sicherzustellen, dass seine Mitarbeiter zusätzlich zu den Regeln und Grundsätzen in diesem Dokument und der zugrunde liegenden vertraglichen Vereinbarung auch die Fernarbeitsrichtlinien nach dem Stand der Technik des Geschäftspartners einhalten (z.B. durch Sensibilisierungstrainings für sicheres Arbeiten von zu Hause).

2. Regeln und Grundsätze

2.1. Schulung des Geschäftspartnerpersonals

Zur Erfüllung der vertraglichen Verpflichtungen soll der Geschäftspartner nur Personal engagieren, das auf dem Stand der Technik der Informationssicherheit (und ggf. sicherer Programmierung) ausgebildet ist, und sicherstellen, dass deren Wissen regelmäßig (mindestens einmal pro Kalenderjahr) aufgefrischt wird.

¹ "Informationen" bedeutet in hier Informationen oder Daten (nicht zugänglich im öffentlichen Bereich), die auf Grundlage aller Arten und Formaten, einschließlich digitaler Formate (z.B. Daten, die auf elektronischen oder optischen Medien gespeichert sind) oder physischer (z.B. Papier), numerischer, audiovisueller, grafischer, kartografischer, narrativer oder immaterieller Formate (z.B. Know-how), erhalten, erzeugt, ausgetauscht, gesammelt oder gespeichert werden und entweder im Besitz von Siemens Energy sind oder im Auftrag von Siemens Energy' Kunden und Lieferanten verarbeitet werden und dem Geschäftspartner zugänglich sind.

Die Geschäftspartner machen sich mit den Informationssicherheitsrichtlinien, -standards und -vorgaben von Siemens Energy vertraut und nehmen auf Verlangen von Siemens Energy an Schulungen zur Informationssicherheit teil.

Der Geschäftspartner wird Siemens Energy im Voraus informieren, wenn Personal ausgetauscht wird, welches für die Erfüllung der vertraglichen Verpflichtungen benötigt wird.

2.2. Umgang mit Informationen

Der Geschäftspartner nutzt die von Siemens Energy bereitgestellten Kommunikations- und Kollaborationslösungen für den Austausch von Informationen (siehe Anhang 1 „Secure Data Communication“), sofern zwischen den Parteien nichts anderes vereinbart ist.

Jedwede Form der Verschleierung oder Fälschung der Identität oder der Bedeutung von verwendeten Informationen durch den Geschäftspartner ist verboten.

2.2.1. Schutz von Informationen

Alle Informationen sind unabhängig von ihrer Erscheinungsform und ihrem Informationsträger gemäß ihrer Einstufung vor Verlust der Vertraulichkeit, Integrität und Verfügbarkeit zu schützen.

Für Informationen von Siemens Energy sind drei Schutzklassen vorgesehen: „Intern“, „Vertraulich“ und „Streng vertraulich“. Entsprechend der Schutzklasse sind bei der Kennzeichnung/Erstellung, Verteilung, Versand und Übertragung, Aufbewahrung und Speicherung sowie bei der Entsorgung/Vernichtung/Löschung Schutzmaßnahmen erforderlich, die mit zunehmendem Schutzbedarf höher werden.

Der Geschäftspartner legt in Absprache mit dem Ansprechpartner bei Siemens Energy den Vertraulichkeitsgrad der von ihm erstellten Informationen fest. Bei überlassenen Informationen ist der Geschäftspartner verpflichtet, die von Siemens Energy definierten Schutzmaßnahmen einzuhalten.

Informationen dürfen nur auf IT-Systemen, -Applikationen und Dateiablagensystemen gespeichert und verarbeitet werden, die einen adäquaten Schutz dieser Informationen gewährleisten, d.h. Informationen mit Schutzklasse "Vertraulich" sind verschlüsselt zu speichern und zu transferieren, während Informationen mit der Schutzklasse "Streng vertraulich" durchgehend (Ende-zu-Ende) verschlüsselt sein müssen.

Der Geschäftspartner darf ohne vorherige Zustimmung von Siemens Energy oder ohne anderweitige vertragliche Vereinbarung zwischen den Parteien weder Kopien noch Vervielfältigungen von Informationen erstellen, löschen, untersuchen oder modifizieren.

2.2.2. Übermittlung von E-Mails

Der sichere Austausch von E-Mails bezieht sich auf E-Mail-Korrespondenz, die von oder zwischen Mitarbeitern und Auftragnehmern des Geschäftspartners, IT-Systemen, Anwendungen und Siemens Energy stammt.

E-Mails, die die Integrität und Vertraulichkeit der Informationen und die Identifizierung des Absenders gewährleisten müssen, sind, unter Einhaltung von Standards nach dem Stand der Technik (z. B. NIST SP800-177R1, TN-1945 oder BSI ISi-Mail-Server), digital zu signieren und Ende-zu-Ende zu verschlüsseln, sofern sie Informationen mit den Schutzklassen "Vertraulich" oder "Streng vertraulich" beinhalten (siehe Anhang 1 "Secure Data Communication").

Dies umfasst z.B. folgenden Informationsaustausch:

- E-Mails mit kommerziellen oder rechtlichen Auswirkungen
- E-Mails, die eine Benutzerinteraktion bedürfen
- E-Mails, die sich auf den Austausch kritischer Sicherheitsinformationen beziehen
- E-Mails, die potenzielle schädliche Inhalte enthalten (z. B. URLs, Anhänge)

Die automatische Weiterleitung eingehender E-Mails an externe Postfächer, E-Mail-Spam, Missbrauch von Siemens Energy-E-Mail-Adressen (z.B. Hinzufügen von E-Mails zu Mailinglisten ohne ausdrückliche Zustimmung) sowie die Übermittlung vertraulicher oder streng vertraulicher Informationen per Fax ist untersagt.

2.2.3. Löschung von Informationen

Der Geschäftspartner hat alle Informationen auf allen seiner Informationsträger, die für die Erbringung der vertraglich vereinbarten Aufgaben oder Tätigkeiten nicht mehr benötigt werden, zuverlässig zu löschen, es sei denn, die Aufbewahrung ist vertraglich vereinbart oder nach den geltenden Gesetzen und Vorschriften erforderlich.

Informationen, die in elektronischer oder Papierform vorliegen, werden in Abhängigkeit von ihrer Vertraulichkeit unter Beachtung von Standards nach dem Stand der Technik (z.B. BS EN 15713 – Schutzstufe 6, NIST SP800-88, DIN 66399-2) gelöscht, bereinigt und entsorgt (d.h. Informationen mit Schutzklassen "Vertraulich" oder "Streng vertraulich" sind unwiederbringlich zu vernichten).

2.3. Zugangs- und Zutrittsberechtigungen

Bei Bedarf und wenn nicht anderweitig zwischen den Parteien vereinbart, soll, in Abhängigkeit der Schutzstufe des jeweiligen IT-Systems, der jeweiligen Anwendung und des jeweiligen Netzwerks, der Geschäftspartner Zugriff ausschließlich über Siemens Energy Zugangslösungen auf das Netzwerk und die Informationen von Siemens Energy erhalten (z.B. über die angebotene Geschäftspartnerzugangslösung von Siemens Energy).

Der Geschäftspartner muss seinen Zugang zu Siemens Energy protokollieren und jede Verbindung zwischen dem Intranet von Siemens Energy und seiner Umgebung vor dem Zugriff von Dritten schützen.

Der Geschäftspartner darf erhaltene Systemzugangs- und Zulassungsberechtigungen (z.B. Passwort- oder Zugangskarten) nur zur Erfüllung seiner vertraglich vereinbarten Aufgaben und Tätigkeiten nutzen. Solche Systemzugangs- und Zulassungsberechtigungen sind auf den Grundsätzen "least privilege", "need to know" und "segregation of duties" anzuwenden.

Der Geschäftspartner wird Siemens Energy zeitnah informieren, wenn sich Änderungen bzgl. der Mitarbeiter oder Subunternehmer mit entsprechendem Zugang zu Informationen ergeben.

Die Zulassungen, alle damit verbundenen technischen Konfigurationen oder kryptografischen Materialien sind vertraulich zu behandeln und dürfen weder an Dritte weitergegeben noch veröffentlicht werden.

Der Geschäftspartner darf diese Zugangslösung und die damit verbundenen Sicherheitsmechanismen nicht umgehen oder missbrauchen.

2.4. Schutz von Systemen und des Datenzugriffs

IT-Systeme und Informationsträger, die von den Geschäftspartnern genutzt oder von Siemens Energy zur Erfüllung der vertraglichen Verpflichtungen zur Verfügung gestellt werden, müssen durch Maßnahmen nach dem Stand der Technik vor unbefugtem Zugriff geschützt werden, einschließlich der physischen Sicherheit für die Arbeitsumgebung des Geschäftspartners.

2.4.1. IT-Systeme und Informationsträger von Siemens Energy

IT-Systeme und Informationsträger von Siemens Energy werden auf der Grundlage von Siemens Energy-Regeln und -Vorschriften gesichert und regelmäßig überwacht. Solche Sicherheitsmaßnahmen dürfen vom Geschäftspartner nicht umgangen oder manipuliert werden. Bei der Nutzung solcher IT-Systeme und Informationsträger lässt der Geschäftspartner die gebotene Sorgfalt walten, was zumindest die folgenden Schutzmaßnahmen umfasst:

- Nutzung des Diebstahlschutzes für mobile Systeme.
- Kein Missbrauch oder unberechtigter Zugriff bei der Nutzung von gemeinsamen Ressourcen.
- Verwendung von unterschiedlichen Passwörtern pro Benutzerkonto (Anonyme- und Gast-Zugänge sind zu deaktivieren).
- Zugriffsrechte dürfen ohne vorherige Zustimmung von Siemens Energy nicht erhöht werden.
- Ausschalten von sprachgesteuerten Smart Devices oder etwaigen Webcams im Arbeitsbereich, die nicht für dienstliche Zwecke benötigt werden (z.B. Amazon Alexa, Apple Siri).
- Abmelden und sicheres Aufbewahren der Geräte, wenn sie nicht genutzt werden.

- Papierdokumente mit vertraulichen oder streng vertraulichen Informationen dürfen nicht offen zugänglich sein oder unbeaufsichtigt bleiben. Sie müssen unter Benutzung geeigneter Schutzmechanismen weggeschlossen werden.

2.4.2. IT-Systeme und Informationsträger im Eigentum des Geschäftspartners

In Ergänzung zu Abschnitt 2.4.1 sind die folgenden zusätzliche Mindestschutzmaßnahmen für IT-Systeme und Informationsträger im Eigentum des Geschäftspartners umzusetzen:

- Installation der aktuellen Bios-Version und Aktivierung des Bios-Passworts.
- Keine Nutzung von dauerhaft lokalen Administrationsrechten.
- Aktivierung des Bildschirmschoners des Betriebssystems mit Passwortschutz (als Systemsperre für unbeaufsichtigte IT-Systeme).
- Aktivierung von Festplatten- und Dateiverschlüsselung.
- Schutz vor Viren und ähnlicher Schadsoftware nach dem Stand der Technik, sofern die IT-Systeme oder Informationsträger solchen Risiken ausgesetzt sind. Für PC-Systeme ist ein aktueller und permanent aktiver Virenschutz einschließlich eines „Endpoint Detection and Response Agents“ zu verwenden.
- Absicherung des Netzwerkzugangs mindestens durch ein Passwort zum Schutz vor unerlaubtem und böartigem Netzwerkverkehr (z. B. Whitelisting).
- Keine Verwendung von Standard-Passwörtern. Löschung von Initialpasswörtern nach Erhalt und Verfall nach 24 Stunden.
- Passwörter müssen aus einer Kombination von Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen erstellt werden. Passwörter müssen mindestens 12 Zeichen enthalten (26 Zeichen für Administratorkonten). Für PINs sind frei wählbare Ziffern zu verwenden. Passwörter müssen alle 180 Tage (45 Tage für privilegierte Administratorkonten) geändert werden, es sei denn, das Passwort ist Teil einer Zwei-Faktor-Authentifizierung. Die letzten 10 Passwörter dürfen nicht wiederverwendet werden.
- Für den Zugriff auf vertrauliche und streng vertrauliche Informationen ist eine Zwei-Faktor-Authentifizierung erforderlich.
- Während des Zugriffs auf Siemens Energy IT-Systeme und Netzwerke darf keine zusätzliche Internetverbindung des Geräts möglich sein.
- Keine Verwendung von Netzwerk- oder Systemanalysegeräten ohne die ausdrückliche vorherige Genehmigung von Siemens Energy.
- Angeschlossene Netzwerkgeräte und darauf eingesetzte Software von Drittanbietern müssen regelmäßig gewartet werden und der Geschäftspartner muss sicherstellen, dass der aktuelle Patch-Level eingespielt ist.

2.5. Informationspflichten, Cybersecurity Kontakt, Kontrolle

2.5.1. Informationspflichten

Der Geschäftspartner informiert die definierten Ansprechpartner von Siemens Energy (u.a. Cybersecurity-Ansprechpartner, Vertragsinhaber) über Betriebsstörungen, Feststellung von Fehlern und Schadensfaktoren (z.B. Computerviren, Programmstörungen) in allen für die Zusammenarbeit genutzten IT-Systemen, Anwendungen, Netzwerken oder Software.

Stellt der Geschäftspartner Schwachstellen oder Sicherheitsvorfälle fest oder liegt ein entsprechender Verdacht vor, wird Siemens Energy unverzüglich darüber informiert, z. B. bei Verdacht auf Missbrauch oder Offenlegung von PINs/Passwörtern.

2.5.2. Cybersecurity Kontakt

Neben den jeweiligen Siemens Energy-Ansprechpartnern ist in den folgenden Fällen die entsprechenden Siemens Energy cybersecurity-Kontaktadresse unverzüglich zu informieren, sofern potenziell oder tatsächlich eine Verletzung von Informationen, IT-Systemen, Applikationen, Netzwerk oder Informationsträgern vorliegt:

cybertprm@siemens-energy.com

2.5.3. Kontrolle

Siemens Energy behält sich das Recht vor, die Einhaltung dieser Regeln und Grundsätze durch den Geschäftspartner wie hier beschrieben zu überwachen. Die an die Netzwerke von Siemens Energy angeschlossenen IT-Systeme werden nach dem Stand der Technik auf Sicherheitslücken geprüft. Identifizierte Schwachstellen müssen vom Geschäftspartner unverzüglich behoben werden. Alle sicherheitsrelevanten Patches und Hotfixes, die von Dritten freigegeben werden, müssen installiert werden, sofern sie im Zusammenhang mit den vertraglichen Verpflichtungen stehen.

Der Geschäftspartner hat darüber hinaus die Einhaltung der hier festgelegten Regeln und Grundsätze in geeigneter Weise zu protokollieren und zu überwachen und dabei die gesetzlichen Vorgaben (z.B. Aufbewahrungsfristen) zu beachten.

Verstößt der Geschäftspartner gegen die hierin enthaltenen Regeln und Grundsätze, kann dies zur Sperrung seines Zugangs zu den Standorten und IT-Systemen von Siemens Energy führen und vertragliche oder rechtliche Konsequenzen nach sich ziehen.

2.6. Beendigung der Zusammenarbeit

Bei Beendigung der Geschäftsbeziehung mit Siemens Energy, einschließlich der Beendigung der Geschäftsbeziehung mit einem Mitarbeiter des Geschäftspartners, und sofern nicht anders vereinbart oder von Siemens Energy verlangt, sind die folgenden Aktivitäten vom Geschäftspartner durchzuführen und schriftlich zu bestätigen:

- Rückgabe aller IT-Systeme, Geräte, Informationen, Informationsträger, Papierunterlagen und Arbeitsmittel (inkl. Zugangskarten).
- Rückgabe aller gewährten Zugänge und Angabe zum Zwecke der Deaktivierung oder Löschung (z.B. Zugang zu Dateifreigaben, Service-Accounts, etc.).
- Löschung von Informationen auf allen Informationsträgern und Vernichtung von Papierdokumenten gemäß Ziffer 2.2.3.
- Deinstallation der von Siemens Energy zur Erbringung der vertraglichen Leistung zur Verfügung gestellten Software (z.B. Virtual Client Software).

Cybersecurity Card

Secure Data Communication

IT Services for Secure Communication and Collaboration of external Business Partner with Siemens Energy

Use Case	Once Secure document exchange	Continuous secure document exchange	Continuous secure data and document exchange	Secure collaboration		Secure collaboration around PLM	Real Time Collaboration
	"We want to exchange <u>once a document</u> securely."	"We want to exchange <u>continuously documents</u> securely."	"We want to exchange <u>continuously data and documents</u> securely."	"We want to work jointly on the <u>same documents</u> ."		"We want to work on <u>same docs / data</u> in PLM area, incl. Integrated, complex scenarios (e.g. Digital Twin)."	"We want to make a <u>secure virtual meeting</u> ."
Recommended IT Service	<u>Secure File Exchange (SecuFEx)</u>	<u>SmartStorage (Syncplicity) / OneDrive</u>	<u>E-Mail Encryption</u>	<u>SharePoint Global Collaboration Service-Portal</u>	<u>Workspace Strictly Confidential / Secure Data Room (SDR)</u>	<u>Siemens Teamcenter (TC)</u>	Real Time Collaboration (RTC) Service <u>MS Teams</u>
Max. Protection Class	"Confidential"	"Confidential"	"Strictly Confidential"	"Confidential"	"Strictly Confidential"	"Confidential" ¹	"Confidential" ²
Technical Prerequisites	<ul style="list-style-type: none"> A temporary user account for sending files must be created by the Siemens Energy business partner contact. 	<ul style="list-style-type: none"> User account at <u>Syncplicity</u> User account at <u>OneDrive</u> 	<ul style="list-style-type: none"> <u>Prerequisites</u> <u>Implementation Guide of Email encryption</u> 	<ul style="list-style-type: none"> <u>Technical prerequisites</u> PC settings Mobile phone or token for authentication 	<ul style="list-style-type: none"> Mobile phone for authentication 	<ul style="list-style-type: none"> <u>TC Supplier Collaboration Foundation (SCF)</u> 	<ul style="list-style-type: none"> Meeting shall be provided by Siemens Energy contact
User instructions and technical contacts	<ul style="list-style-type: none"> <u>SecuFEx Website</u> 	<ul style="list-style-type: none"> <u>Syncplicity Website</u> <u>OneDrive Website</u> 	<ul style="list-style-type: none"> <u>Siemens PKI Website</u> 	<ul style="list-style-type: none"> <u>SharePoint Global Collaboration Service Portal Website</u> 	<ul style="list-style-type: none"> <u>SDR Website</u> 	<ul style="list-style-type: none"> <u>Teamcenter</u> 	<ul style="list-style-type: none"> <u>MS Teams</u>

Version for externals

¹ Depends on local installation and configuration, maximum up to "Restricted". Exact Protection Class needs to be verified with your Siemens contact.

² MS Teams can use with max. protection class "Confidential".

Restricted © Siemens Energy 2020, SE CYS GOV, version 2.0, 19.01.2021

Cybersecurity Card

Secure Data Communication

SIEMENS
energy**Definition**

Business Partner (BP): in this context it is every external party with a business relationship to Siemens, without authorized access to Siemens Intranet (e.g. via [Business Partner Access](#)) and therefore with no access to Siemens internal IT Services.

Situation

The exchange of information with Business Partners is our daily business. In some cases, data and documents (like costs, contracts or technical documents) are classified as "confidential" or even "strictly confidential". To ensure secure communication and collaboration of such information, this use case based IT Service overview has been created. It helps Siemens end user as well as their Business Partners to identify the respectively adequate Siemens IT Service, to know where to order it and how to use it. Please, be aware that IT Services for specific business processes (e.g. electronic data interchange via [EDI](#)) are still leading and the overview should only cover remaining use cases (e.g. for which so far unencrypted email process has been used).

Threat

Non Disclosure Agreements (NDAs) and the Siemens "[Rules for Business Partners](#)" define the right handling of confidential information, but do not contain concrete IT solutions for the implementation of the regulations.

That leads to the risk that, although the Information Security requirements are known, they might not be implemented correctly or completely.

Behavior**What to consider as a business partner when sending an email with SecuFEx:**

The Business Partner needs a temporary account for SecuFEx to send data to a Siemens employee. This temporary account can be created and administrated by each Siemens employee. Users of the SecuFEx service shall comply with all applicable national and international (re-) export control regulations.

What to consider as a business partner when receiving a virtual conference or Circuit invitation from a Siemens employee:

The Business Partner must ensure that there are no prying eyes and eavesdroppers in the virtual meeting. Furthermore, the Business Partner is not allowed to make hardcopies from the screen, if confidential information is shown. During virtual meeting sessions open only those applications and documents that are relevant to your respective meeting and avoid sharing the complete desktop. Furthermore, no confidential documents shall be uploaded to the virtual meeting server.

This list highlights important topics.

Please note, however, that the list is not exhaustive and that all general cybersecurity regulations also apply.

Further Information**Siemens Energy Global Website:**

<https://www.siemens-energy.com/global/en.html>

Supplier at Siemens Energy:

<https://www.siemens-energy.com/global/en/company/about/supply-chain-management/supplier-information.html>

Siemens Energy Condition of Purchase:

<https://www.siemens-energy.com/global/en/company/about/supply-chain-management/supplier-information.html>

Cybersecurity Contacts: <https://wiki.siemens-energy.com/display/cys/SE+Cybersecurity+Contacts>

Further Cybersecurity Cards on other topics:

<https://wiki.siemens-energy.com/display/cys/Cybersecurity+Cards>