SIEMENS

Be aware, be secure

Informationssicherheit

Regelungen für Geschäftspartner

Datum:	2015-08-21
Version:	1.0
Eigener/Eigentümer:	Siemens Chief Information Security Officer
Veröffentlicht von:	GS IT ISEC

1. Anwendungsbereich

Die Regelungen für Geschäftspartner gelten für Geschäftspartner von Siemens, die im Rahmen eines Vertragsverhältnisses Zugang oder Zugriff auf IT-Systeme, -Applikationen, -Netze oder firmenvertrauliche Informationen[1] von Siemens haben.

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

1.1. Verantwortlichkeiten

Dem Geschäftspartner von Siemens wird zur Erfüllung vertraglicher Verpflichtungen und zur Steigerung der Effizienz der Geschäftsabwicklung Zugang und Zugriff auf Informationen bzw. IT-Systeme, -Applikationen und -Netze oder firmenvertrauliche Informationen von Siemens ermöglicht.

Dies bedarf Maßnahmen zum Schutz der IT-Systeme, -Applikationen, -Netze und firmenvertraulichen Informationen vor ungewollter Offenlegung, unberechtigten Zugriff, Manipulation, Computerviren, Hacking, Cypberangriffen und anderer Bedrohungen. Dazu ist es erforderlich, dass Geschäftspartner von Siemens die nachfolgenden Regeln und Grundsätze einhalten und Schutzmaßnahmen weder außer Betrieb nehmen, umgehen oder in sonstiger Weise verändern.

Der Geschäftpartner verpflichtet sich zusätzlich zu den sonstigen vertraglichen Vereinbarungen, die hierin definierten Regeln und Grundsätze zu beachten sowie diese Unterlage seinen Mitarbeitern, die Zugang oder Zugriff auf IT-Systeme, -Applikationen und -Netze von Siemens oder firmentvertrauliche 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.

2. Regeln und Grundsätze

2.1. Umgang mit Informationen

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

Firmenvertrauliche Informationen von Siemens sind alle Informationen, die nicht öffentlich sind. Für firmenvertrauliche Informationen sind drei Schutzklassen vorgesehen: „Intern“, „Vertraulich“ und „Streng vertraulich“. Entsprechend der Schutzklasse sind bei der Kennzeichnung/Erstellung, Verteilung, dem Versand und der 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 den Vertraulichkeitsgrad der von ihm erstellten Informationen fest. Bei überlassenen Informationen ist der Geschäftspartner verpflichtet, die von Siemens definierten Schutzmaßnahmen einzuhalten.

Firmenvertrauliche Informationen dürfen nur auf IT-Systemen, -Applikationen und Dateiablagesystemen gespeichert und verarbeitet werden, die einen adäquaten Schutz dieser Informationen gewährleisten.

[1] Informationen von Siemens können in allen Medien und Formen vorliegen, einschließlich in digitaler Form (z.B. Dateien, die auf elektronischen oder optischen Medien gespeichert sind), in materieller Form (z.B. auf Papier), numerisch, audiovisuell, grafisch, kartografisch, erzählend, als auch als immateriell in Form von Kenntnissen.

Der Geschäftspartner ist verpflichtet, die verschüsselte Übertragung von E-Mails (mit vertraulichem oder streng vertraulichem Inhalt) und die Entschlüsselung empfangener verschlüsselter E-Mails zu ermöglichen.

Die automatische Weiterleitung empfangener E-Mails an externe Postfächer ist ebenso untersagt wie der Faxversand von vertraulichen und streng vertraulichen Informationen.

Informationen von Siemens, die für die Erbringung der vertraglich vereinbarten Aufgaben und Tätigkeiten nicht mehr erforderlich sind und nicht aufgrund gesetzlicher oder vertraglicher Aufbewahrungspflichten vorgehalten werden müssen, sind vom Geschäftspartner zuverlässig von allen seinen Informationsträgern zu löschen. Während eines normalen Arbeitsablaufes dürfen auf IT-Systemen gespeicherte elektronische Informationen mit den vom IT-System standardmäßig angebotenen Löschfunktionen gelöscht werden, wenn eine Verschlüsselung eingerichtet ist. Wurde keine Verschlüsselung eingerichtet, müssen Informationen mit einer adäquaten Methode, vergleichbar zum Standard DOD 5220.22-M, gelöscht werden.

Papierdokumente sind mit Hilfe eines geeigneten Aktenvernichters der Sicherheitsstufe / Level 6 nach EN 15713:2009 oder durch einen Entsorgungsdienst zu vernichten. Wenn der Geschäftspartner keine geeigneten Entsorgungsmöglichkeiten bzw. Aktenvernichter hat, muß das weitere Vorgehen mit dem Ansprechpartner bei Siemens abgesprochen werden (z.B. Nutzung von Siemens-internen Einrichtungen).

2.2. Zugangs- und Zutrittsberechtigungen

Soweit der Geschäftspartner Zugangs- und/oder Zutrittsberechtigungen (z.B. Passwort oder Zugangskarten) erhält, sind diese nur in dem Umfang zu nutzen, wie dies zur Erfüllung seiner vertraglich vereinbarten Aufgaben und Tätigkeiten notwendig ist. Diese sind vertraulich zu behandeln und dürfen weder an Dritte weitergegeben noch offengelegt werden.

2.3. Zugangs- und Zugriffsschutz

Die vom Geschäftspartner für die Erfüllung der Aufgaben benutzten IT-Systeme und Informationsträger sowie alle von Siemens an den Geschäftspartner übergegebenen IT-Systeme und Informationsträger sind nach aktuellem Stand der Technik wirksam gegen den Zugang und Zugriff durch Unbefugte zu schützen. Folgende Maßnahmen gelten aus heutiger Sicht zum Mindestschutz für IT-Systeme und Informationsträger:

- Bios-Passwort.
- Bildschirmschoner mit Passwortschutz des Betriebssystems (als Systemsperre bei unbeaufsichtigten IT-Systemen).
- Diebstahlschutz bei Mobilsystemen.
- Festplatten- und Dateiverschlüsselung.
- Schutz vor Viren und ähnlicher Schadsoftware nach aktuellem Stand der Technik, soweit die IT-Systeme oder Informationsträger solchen Risiken unterliegen. Für PC-Systeme sind aktuelle, permanent wirkende Virenwächter einzusetzen.
- Absicherung von Netzzugängen mindestens durch Passwort.
- Keine Zugriffsmöglichkeiten Unbefugter durch Ressourcen-Sharing.
- Verwendung eines eigenen unterschiedlichen Passworts je Benutzerkonto.
- Keine Verwendung von Standardpasswörtern. Löschung von Initialpasswörtern sofort nach deren Erhalt.
- Passwörter müssen aus einer Kombination von Klein- und Großbuchstaben, Zahlen und Sonderzeichen gebildet werden. Passwörter müssen mindestens 8 Zeichen (bei administrativen Kennungen 16 Zeichen) enthalten. Für PINs müssen Zufallszahlen verwendet werden. Passwortwechsel sind mindestens alle 90 Tage (bei administrativen Kennungen 30 Tage) vorzunehmen. Die letzten 10 Passwörter sind nicht wieder zu verwenden.
- Papierdokumente und mit vertraulichen oder streng vertraulichen Dokumenten dürfen nicht offen zugänglich und unbeaufsichtigt sein. Diese müssen mit geeigneten Schutzmechanismen weggeschlossen werden.

2.4. Informationspflichten, Kontrolle

Die von Siemens und dem Geschäftspartner definierten Ansprechpartner informieren sich gegenseitig und rechtzeitig über relevante Betriebsstörungen, bei Erkennung von Fehlern und Schadensfunktionen in allen innerhalb der Zusammenarbeit genutzten IT-Systemen, -Applikationen, -Netzen oder Software (z.B. Computerviren, Programmfehler).

Sofern der Geschäftspartner Schwachstellen und Vorfälle mit möglicher Auswirkung auf die Informationssicherheit erkennt, z.B. Verdacht eines Missbrauchs oder Offenlegung von PINs/Passwörtern, müssen diese unverzüglich dem Ansprechpartner bei Siemens gemeldet werden.

Der Geschäftspartner ist zur Einhaltung von Hinweisen und Regelungen seitens Siemens zur Sicherheit der IT-Systeme , -Applikationen und -Netze verpflichtet. Eine personalrechtliche oder disziplinarische Weisungsbefugnis gegenüber dem Geschäftspartner besteht nicht.

Die Einhaltung dieser Regeln und Grundsätze zur Informationssicherheit wird bei Siemens kontrolliert. Die an die Netze von Siemens angeschlossenen IT-Systeme werden gemäß dem Stand der Technik auf Sicherheitsschwachstellen hin überprüft. Identifizierte Schwachstellen müssen vom Geschäftspartner unverzüglich behoben werden. Von den Herstellern angebotene sicherheitsrelevante Patche, Korrekturen und Hotfixe müssen vom Geschäftspartner installiert werden.

Falls der Geschäftspartner einzelne oder alle der vorliegenden Regeln missachtet, kann dies zur Sperrung von Zugangs- bzw. Zutrittsberechtigungen zu den Räumlichkeiten von Siemens bzw. von Zugriffsberechtigungen zu Siemens IT-Systemen führen sowie vertraglich vereinbarte bzw. gesetzlich normierte Konsequenzen nach sich ziehen.

2.5. Beendigung der Zusammenarbeit

Bei Beendigung der Zusammenarbeit mit Siemens werden, sofern nichts anderes vereinbart wurde, vom Geschäftspartner folgende Tätigkeiten ausgeführt und schriftlich bestätigt:

- Rückgabe aller überlassenen IT-Systeme, Geräte, Informationen, Informationsträger, Papierdokumente und Arbeitsmittel.
- Rückgabe aller erteilten Zutritts- oder Zugangsberechtigungen sowie Nennung aller Zugriffsberechtigungen zwecks Deaktivierung bzw. Löschung (z.B. Zugriffberechtigungen auf Dateiablagen).
- Löschung von Informationen auf allen Informationsträgern und Vernichtung von Papierdokumenten gemäß Kapitel 2.1.

2.6. Zusätzliche Regeln für Geschäftspartner mit Anschluss zu Siemens IT Systemen, -Applikationen und -Netzen

Der Geschäftspartner verpflichtet sich, den Anschluss nur in der mit Siemens vereinbarten technischen Konfiguration und an den dafür vorgesehenen IT-Systemen zu betreiben.

Informationen über Strukturen, Zugangsmöglichkeiten (z.B. Netzadressen) und Sicherheitsvorkehrungen der Siemens IT-Systeme, -Applikationen und -Netze sind firmenvertrauliche Informationen (vgl. Kapitel 2.1) und sind vom Geschäftspartner dementsprechend zu behandeln.