Vorgaben zur Informationssicherheit syracom AG

*****Englisch Version below*****

Inhalt

Informationssicherheitspolitik 3
Einführung 3
Leitbild 3
Ziele 4
Schutzziele der Informationssicherheit 4
Verpflichtung zur fortlaufenden Verbesserung 4
Anforderung Lieferanten 6
Informationsklassifizierung 6
Meldung von Informationssicherheitsvorfällen 8
Definitionen 9
Beispiele Meldungen (Auszug) 10

……****Englisch Version**** 11

Requirements for Information Security at syracom AGInformation Security Policy 11
Introduction 12
Mission Statement 12
Goals 13
Goals for protecting the Information Security 13
Commitment to continuous Improvement 13
Requirements for Suppliers 15
Information for Classification 15
Reporting Information Security Incidents 17
Definitions 18
Example Notifications (Excerpt) 19

Informationssicherheitspolitik

Einführung

Informationen sind die grundlegenden Bestandteile aller Geschäftsprozesse der syracom AG und damit existentiell bedeutende Unternehmenswerte. Zweck dieser Leitlinie ist es, externe Lieferanten sowie interessierte Parteien über das Ziel zu informieren und unternehmensrelevante Informationen gemäß ihrer Schutzbedarfe angemessen zu schützen. Der Schutz dieser Werte ist unverzichtbar, um die Leistungsfähigkeit und Wettbewerbsposition des Unternehmens sowie das Vertrauen bei Geschäftspartnern und Kunden zu erhalten und zu verbessern. Darüber hinaus erstreckt sich der Schutz von Informationen auf alle Geschäftsprozesse und Geschäftsfelder, unabhängig von Unternehmensstrukturen und Ländergrenzen. Dabei sind alle Formen von Informationen und jegliche Art der Nutzung von Informationen zu schützen.

Die syracom

- sorgt für sicheren Umgang mit Informationen im Allgemeinen.
- ist sich der Bedeutung der Informationssicherheit für das Unternehmen, seine Partner, Lieferanten und Kunden bewusst.
- trifft systematische Vorkehrungen zur Reduzierung von Risiken.
- legt klare Verantwortlichkeiten für die Informationssicherheit fest.
- schützt eigene und anvertraute Informationen vor unberechtigter Kenntnisnahme und unberechtigter Veränderung.
- sorgt für sichere Entwicklung und den sicheren Betrieb von IT-Systemen.
- sorgt für sichere Nutzung von Informationen durch Geschäftspartner.
- schreibt eine strikte und nachvollziehbare Vorgehensweise bei Informationssicherheitsvorfällen vor.
- trifft alle Vorkehrungen zur Fortführung des Geschäftsbetriebes bei Ausfall von Informationssystemen.
- sorgt für einen kontinuierlichen Verbesserungsprozess - unter anderem durch den Einsatz eines Informationssicherheitsmanagementsystems (ISMS).
- schreibt diese Regelungen zur Informationssicherheit fest und kommuniziert diese an Mitarbeiter, Lieferanten, Geschäftspartner sowie weitere interessierte Parteien.

Leitbild

Ziel des Informationssicherheitsmanagements ist es, die Verfügbarkeit, Integrität und Vertraulichkeit aller für Geschäftsprozesse erforderlichen Informationen zu gewährleisten, um einen anhaltenden geschäftlichen Erfolg und einen kontinuierlichen Geschäftsbetrieb sicherzustellen. Daher erfolgt die Sicherstellung der Informationssicherheit im ureigenen Interesse von syracom, aber auch im Sinne von deren Kunden, Mitarbeitern und Geschäftspartnern.

Dieses Ziel kann jedoch nur erreicht werden, wenn angemessene Sicherheitsstandards definiert und erfolgreich umgesetzt werden. Die Geschäftsführung der syracom verpflichtet

sich daher, diese Standards der Informationssicherheit einzuhalten, sie ständig weiterzuentwickeln und durch Qualitätssicherungsmaßnahmen zu überwachen, um neue oder veränderte Risiken frühzeitig identifizieren, analysieren und mit geeigneten Gegenmaßnahmen begegnen zu können.

Ziele

Die syracom betreibt ein ISMS mit dem Zweck der Messung, Beherrschung und Minimierung von Risiken mit Bezug zur Informationssicherheit.

Die Informationssicherheit von syracom orientiert sich an strategischen Zielen, welche im Leitbild und Unternehmenskultur (syracom.de) enthalten sind.

Die Weiterentwicklung der syracom steht im Einklang mit einem angemessenen Informationssicherheitsniveau und einem entsprechenden Informationssicherheitsmanagementsystem nach ISO 27001.

Der Ausbau des Informationssicherheitsmanagements trägt durch die verbesserte Sicherheit zum Unternehmenserfolg bei. Bei der Planung, der Gestaltung, der Überwachung und der Steuerung von Informationen und Kommunikationen werden die Vorzüge bestehender Geschäftsprozesse berücksichtigt.

Schutzziele der Informationssicherheit

Um Beeinträchtigungen der Informationssicherheit zu minimieren, ist das Management von angemessenen Sicherheitsmaßnahmen unter Berücksichtigung einer großen Bandbreite von Bedrohungen erforderlich.

- syracom schützt ihre eigene Arbeitsfähigkeit, Vertrauenswürdigkeit und Zuverlässigkeit.
- syracom schützt die Vertraulichkeit der verarbeiteten und gespeicherten Daten ihrer Kunden, Geschäftspartner und Mitarbeiter.
- syracom schützt vertrauliche Informationen wie z. B. Geschäftsprozesse, Vertragsdaten oder sonstige Geschäftsgeheimnisse.
- syracom gewährleistet die Verfügbarkeit ihrer IT-Systeme, Programme und Daten.
- syracom schützt die Integrität ihrer IT-Systeme, Programme und Daten.
- syracom verhindert den Missbrauch ihrer IT-Systeme, Programme und Daten zweckwidriger Nutzung, sowie Nutzung durch Unbefugte.

Die Schutzmaßnahmen umfassen technische Maßnahmen (z. B. für Software, Hardware, Konfiguration), organisatorische Vorkehrungen (z. B. verbindliche Regeln und Vorgaben) sowie personelle Maßnahmen (z. B. Schulungen, Mitarbeiterauswahl).

Verpflichtung zur fortlaufenden Verbesserung

Der Informationssicherheitsbeauftragte unterstützt die Geschäftsführung bei der regelmäßigen Überprüfung des Informationssicherheitsmanagementsystems auf Aktualität und Wirksamkeit. Die getroffenen Maßnahmen werden regelmäßig daraufhin geprüft, ob sie

den Personen im Geltungsbereich des Managementsystems bekannt, umgesetzt, in den betrieblichen Prozess integriert sowie wirksam sind.

Alle Mitarbeiter, externe Parteien sowie sonstige interessierte Parteien sind zur ständigen Verbesserung der Informationssicherheit verpflichtet und unterstützen diese. Die Mitarbeiter werden ermutigt, mögliche Verbesserungen oder Schwachstellen zu melden.

Durch eine kontinuierliche Überarbeitung von Richtlinien und der Überwachung deren Einhaltung wird das gewünschte Sicherheits- und Datenschutzniveau gewährleistet. Abweichungen werden mit dem Ziel analysiert, die Situation der Informationssicherheit zu verbessern.

Anforderung Lieferanten

Informationsklassifizierung

Sämtliche Informationen, welche durch den Lieferanten übermittelt werden und Informationen der syracom enthalten, sind entsprechend Ihrer Vertraulichkeit zu handhaben.

Bei der Klassifizierung und den damit verbundenen Sicherheitsmaßnahmen werden die geschäftlichen Anforderungen der syracom AG für die gemeinsame Nutzung oder Einschränkung des Zugangs zu Informationen sowie die gesetzlichen Vorschriften berücksichtigt. Die zugewiesene Vertraulichkeitsstufe ist die führende Klassifizierung der Information.

Vertraulichkeit ist der Schutz vor unautorisierter Offenlegung von Informationen. Als "vertraulich“ gekennzeichnete Informationen dürfen ausschließlich autorisierten Personen in der zulässigen Weise verfügbar sein. Bei der Klassifizierung der Informationen ist folgendes Klassifizierungsschema für die Einstufung der Vertraulichkeitsstufe anzuwenden:

Vertraulichkeitsstufe	Kennzeichnung	Klassifizierungskriterien	Zugangsbeschränkung
Öffentlich	Öffentlich	Die Veröffentlichung der Informationen beeinflusst die syracom nicht	Die Informationen sind öffentlich verfügbar
Interner Gebrauch	Intern	Unberechtigter Zugang zu den Informationen können geringe Schäden für die syracom verursachen	Die Informationen sind für alle Mitarbeiter und ausgewählte Dritte verfügbar
Vertraulich	Vertraulich	Unberechtigter Zugang zu den Informationen können erhebliche Schäden für die syracom verursachen	Die Informationen sind nur für eine spezifische Gruppe von Mitarbeitern und autorisierten Dritten zugänglich
Geheim	Geheim	Unberechtigter Zugang zu den Informationen können katastrophale (irreparable) Schäden für das Geschäft und/oder das Ansehen der syracom verursachen	Die Informationen sind nur für einzelne Mitarbeiter zugänglich

Für alle Informationen und informationsverarbeitenden Einrichtungen ist eine Regelung zur Handhabung, Speicherung und Kommunikation dieser gemäß der Informationsklassifizierung geregelt. Alle Personen mit Zugang zu klassifizierten Informationen müssen die nachstehend aufgeführte Regelung befolgen. Bei Verstößen gegen diese Regelung (z.B. durch Offenlegung an unautorisierte Personen), ist eine Meldung gemäß des Meldeprozesses zwingend erforderlich. Die Handhabung von Werten unterscheidet sich in der Art der Information. Die syracom unterscheidet dabei in “Digitale Informationen” (DI), “analoge Informationen” (AI) und dem “gesprochenen Wort” (GW).

Intern	Vertraulich	Geheim
Kennzeichnung (DI, AI)		
Markierung „Intern“ auf mindestens der ersten Seite des Dokuments	Markierung „vertraulich“ auf jeder Seite des Dokuments	Markierung „geheim“ auf jeder Seite des Dokuments
Speicherung und Aufbewahrung (DI, AI)		
Ablage in O365/ Aufbewahrung im Büro	Ablage in O365 mit einem eingeschränkten Benutzerkreis / Aufbewahrung im verschlossenen Büro oder gesicherter Schublade	Verschlüsselte Ablage in O365 Aufbewahrung im Tresor
Drucken		
Direktes Drucken	PIN-Print	Eigener Drucker im Büro
Löschen und Vernichten (DI, AI)		
Einfaches Löschen Papierkorb im Gebäude	Einfaches Löschen/ Entsorgung über Container	Vernichtung des digitalen Datenträgers, Löschen von Dokumenten im zentralen und lokalen Ablageort, Löschen aus dem Backup/ Entsorgung über Container
Weitergabe (DI, AI, GW)		
Weitergabe nur an berechtigten Personenkreis	Weitergabe nur an berechtigten Personenkreis/ Extern verschlüsselt (DI)	Weitergabe nur nach Genehmigung des Eigentümers und namentlich bekannten Personenkreis/ Immer verschlüsselt (DI)

Für die Zurverfügungstellung von Informationen gilt das need-to-know-Prinzip. Es sind geeignete technische Mittel (z.B. Verschlüsselung) einzusetzen, um ein angemessenes Sicherheitsniveau bei der Übermittlung von Informationen zu gewährleisten. Informationen können über folgende elektronische Kommunikationswege ausgetauscht werden:

- E-Mail
- Übertragung von Daten via OneDrive, SharePoint
- Übertragung von Daten über weitere Anbieter, wie Dropbox, Google Drive, etc.
- Übermittlung von E-Mails und Daten über Secureshare
- (Teams)-telefonie
- Versand von SMS-Textnachrichten

Bei der Übertragung von Informationen muss die Klassifizierung sowie die Handhabung der Informationen berücksichtigt werden.

Folgende Verfahren zur elektronischen Nachrichtenübermittlung sind gestattet:

Schutzbedarf der Art der Information Übertragung	Normal (z.B. öffentlich & intern)	Hoch (z.B. vertraulich)	Sehr hoch (z.B. Geheim)
E-Mail	Ohne Einschränkungen erlaubt	Nur mit Transportverschlüsselung erlaubt	Nur mit Dokumentenverschlüsselung erlaubt
Übertragung von Daten via OneDrive, SharePoint	Ohne Einschränkungen erlaubt	Ohne Einschränkungen erlaubt	Nur mit Dokumentenverschlüsselung erlaubt
Übertragung von Daten über weitere Anbieter, wie Dropbox, Google Drive, etc.	Ohne Einschränkungen erlaubt	Verboten	Verboten
Übermittlung von E-Mails und Daten über Secureshare	Ohne Einschränkungen erlaubt	Ohne Einschränkungen erlaubt	Transportpasswort obligatorisch
(Teams)-telefonie	Ohne Einschränkungen erlaubt	Nur bei Sicherstellung des Personenkreises erlaubt	Nur bei Sicherstellung des Personenkreises erlaubt
Versand von SMS-Textnachrichten	Ohne Einschränkungen erlaubt	Verboten	Verboten

Erhält ein Lieferant zur Durchführung seiner Aufgaben Zugriff auf das Kommunikationsnetz oder auf Komponenten der IT-Infrastruktur der syracom, temporär oder im Rahmen dauerhaft bestehender Dienstleistungsverträge, so sind diesem die innerhalb der syracom geltenden Regeln und Vorschriften zu handhaben. Die für den Lieferanten verantwortliche Person/ Entität, welche den Zugriff beschafft hat darüber aufzuklären. Wurde die Remote-Verbindung nur temporär erteilt, so wird sie umgehend nach erfolgter Leistungserbringung deaktiviert.

Es sind geeignete technische Mittel (z.B. Anmeldeverfahren) einzusetzen, um ein angemessenes Sicherheitsniveau beim Zugriff auf die Komponenten zu gewährleisten.

Um die IT-Infrastruktur vor Störungen zu schützen und die Sicherheit der in ihr verarbeiteten, gespeicherten und übertragenen Informationen zu gewährleisten, wird der Lieferant, welcher Zugriff auf IT-Systeme der syracom hat auf nachfolgende Regelungen verpflichtet:

- Das unrechtmäßige Abrufen oder Verbreiten von Inhalten, die urheberrechtlich geschützt sind, ist untersagt.
- Ebenfalls untersagt ist das Abrufen oder Verbreiten von strafrechtlich relevanten oder sittenwidrigen Inhalten.
- Das eigenmächtige Herunterladen von Software sowie die Installation oder Verwendung nicht freigegebener Hard- und Software ist den Lieferanten oder sonstigen Auftragnehmern nicht gestattet.
- Der Zugriff auf das Internet oder auf Netzwerke, die nicht vom Unternehmen betrieben werden, erfolgt grundsätzlich nur über die vom Unternehmen speziell dafür bereitgestellten Zugänge.
- Zugangskennungen für die Nutzung der IT-Infrastruktur (wie z.B. Passwörter) sind von einem Lieferanten oder sonstigen Auftragnehmern geheim zu halten und dürfen grundsätzlich nicht an Dritte weitergegeben werden. Auch innerhalb der jeweiligen Organisation des Lieferanten oder sonstigen Auftragnehmern ist dieser verpflichtet, die Daten vor anderen Mitarbeitern des Auftragnehmers geheim zu halten. Ausnahmen hiervon können gemacht werden, wenn die Leistungen des Auftragnehmers von einem Team von Personen für die syracom durchgeführt wird.
- Die private Nutzung von IT-Systemen der syracom ist jedem Lieferanten oder Auftragnehmer untersagt.
- Den Lieferanten sind eigennützige Verarbeitungen von personenbezogenen Daten oder eigennützige Verarbeitungen von schutzbedürftigen Informationen der syracom, auf die ein Lieferant aufgrund seiner Aufgaben Zugriff erhält, nicht gestattet

Meldung von Informationssicherheitsvorfällen

Der Lieferant muss jegliche Ereignisse im Kontext der Informationssicherheit umgehend per E-Mail an Informationssicherheit@syracom.de melden. Hierbei ist der Fokus auf die Informationen der syracom AG zu legen. Sofern der Verlust der Verfügbarkeit, Vertraulichkeit und Integrität der syracom-Informationen gefährdet ist, ist dies zu melden.

Im Rahmen der Meldung sind folgende Informationen anzugeben:

- Was ist passiert?
- Wann ist es passiert, wann ist es aufgefallen?
- Wer war involviert? (waren bei der Auslösung des Vorfalls auch Dritte involviert wie z.B. Projektmitarbeiter?)

- Wen betrifft der Vorfall? (MA von syracom, Bewerber, Kunden, Partner? Wie viele Personen sind ca. betroffen?)
- Wurden bereits Maßnahmen ergriffen?

Definitionen

Informationssicherheitsereignisse sowie Informationssicherheitsvorfälle sind dabei wie folgt definiert:

- **Informationssicherheitsereignis**: Anerkanntes Auftreten eines Zustands eines Systems, Dienstes oder Netzwerks, der eine mögliche Verletzung der Informationssicherheitspolitik oder die Unwirksamkeit von Maßnahmen oder eine vorher nicht bekannte Situation, die sicherheitsrelevant sein kann, anzeigt.

- **Informationssicherheitsvorfall / Incident**: Einzelnes ungewolltes oder unerwartetes Informationssicherheitsereignis oder eine Reihe solcher Ereignisse, die eine erhebliche Wahrscheinlichkeit besitzen, Geschäftstätigkeiten zu gefährden und die Informationssicherheit zu bedrohen.

Informationssicherheits-Incidentmanagement

Nach Eingang einer Meldung, wird das gemeldete Ereignis erstmalig durch den ISB der syracom AG überprüft, um festzustellen, ob ein potenzieller Vorfall besteht. Dabei wird zusätzlich die Zuständigkeit für den Vorfall evaluiert. Wurde keine potenzieller Vorfall festgestellt, erhält der Melder eine Rückmeldung und die Bearbeitung ist abgeschlossen.

Sollte ein potenzieller Informationssicherheitsvorfall erkannt worden sein, wird eine Situationsklärung durch den ISB durchgeführt und der Vorfall sowie alle weiteren Schritte dokumentiert. Das Ziel der Situationsklärung ist es den Vorfall zu bestätigen oder zu entkräften und dabei zudem den Schweregrad des Vorfalls zu ermitteln. Hierfür kann sich der ISB Unterstützung aus allen benötigten Bereichen sowie von dem Melder des Vorfalls heranziehen. Folgende drei Ergebnisse und ihre Kriterien können aus der Situationsklärung kommen:

<u>Keine Relevanz identifiziert</u>

- Informationssicherheitsvorfall kann ausgeschlossen werden
- Vorfall ist bereits vollständig geklärt und es gibt keinen erkennbaren Schaden

<u>Vorfall identifiziert</u>

- Verdacht auf niedrige bis mittlere Auswirkung / Schaden
- Kein Verdacht auf vorsätzliche Handlung

<u>Erheblicher Vorfall identifiziert</u>

- Verdacht auf besonders hohe Auswirkung / Schaden
- Verdacht auf vorsätzliche Handlung bei geringer Auswirkung / Schaden

Darüber hinaus ist zu klären, ob die Sicherheit personenbezogener Daten beeinträchtigt ist. Sollte dies der Fall sein, so ist der Datenschutzbeauftragte einzubinden.

Beispiele Meldungen (Auszug)

- Versehentlicher Versand einer E-Mail mit vertraulichen Informationen an falschen Empfänger
- Verlust des syracom-Endgeräts (Falls zutreffend)
- Verlust der physischen Zugangskarte (Falls Zutreffend)

****Englisch Version****

Requirements for Information Security at syracom AG

Information Security Policy

Introduction

Information is the fundamental component of all business processes at syracom AG and is therefore a vital corporate asset. The purpose of this policy is to inform external suppliers and interested parties of the objective and appropriate protection of company-relevant information in accordance with their protection requirements. Protecting these assets is essential to maintaining and improving the company's performance and competitive position, as well as the confidence of business partners and customers. In addition, information protection extends across all business processes and lines of business, regardless of organizational structure or national boundaries. All forms of information and all uses of information must be protected.

syracom

- ensures safe handling of Information in general.
- is aware of the importance of Information Security for the company, its partners, suppliers, and customers.
- takes systematic precautions to reduce risks.
- defines clear responsibilities for Information Security.
- protects owned and entrusted Information from unauthorized access and unauthorized changes.
- ensures safe development and the secure Operations of IT systems.
- ensures safe usage of Information by business partners.
- adheres to a strict and comprehensible procedure pertaining to Information Security Incidents.
- takes every precaution to ensure business continuity in the event of an information system failure.
- ensures a continuous improvement process – especially through the implementation of an Information Security Management System (ISMS).
- establishes and communicates these information security policies to employees, suppliers, business partners, and other interested parties.

Mission Statement

The goal of Information Security Management is the Confidentiality, Integrity, and Availability of all information needed for business processes to ensure ongoing business success and business continuity. Ensuring information security is therefore in syracom's own interest, as well as in the interest of its customers, employees, and business partners.

This goal can only be achieved if appropriate security standards are defined and successfully implemented. The management of syracom is committed to maintaining and continuously improving these information security standards and to monitoring them through quality

assurance and analysis to identify new or changed risks and to be able to implement appropriate countermeasures.

Goals

Syracom operates an ISMS with the purpose of measuring, control, and minimizing of risks in reference to Information Security.

Information security at syracom is aligned with strategic goals that are embedded in the mission statement and corporate culture (at syracom.de).

The further development of syracom is in line with an appropriate level of Information Security and a corresponding ISMS in accordance with ISO 27001.

The expansion of the ISMS contributes to the company's success through improved security. In the planning, management, and monitoring of information and communication, the benefits of the business processes that are already in place are leveraged.

Goals for protecting the Information Security

To minimize adverse effects of Information Security, the management of appropriate Security measures, while considering a wide range of threats, is required.

- Syracom protects its own ability to work, trustworthiness, and reliability.
- Syracom protects the Confidentiality of the information it processes and stores about its customers, business partners, and employees.
- Syracom protects confidential information such as business processes, contract data, and other business secrets.
- syracom guarantees the Availability of its IT-Systems, Programs, and Data.
- syracom protects the Integrity of its IT-Systems, Programs, and Data.
- syracom prevents the misuse of its IT-Systems, Programs, and Data by preventing improper use and the use by unauthorized parties.

These protection measures encompass technical measures (e.g. for software, hardware, and configuration), organizational precautionary measures (e.g. binding policies and guidelines) as well as personal measures (e.g. Training and selection of Employees).

Commitment to continuous Improvement

The Information Security Officer supports the management during regular inspection of the ISMS to ensure and measure its actuality and effectiveness. The measures taken are regularly validated to ensure that they are known to the people involved in the management

system, that they have been implemented, that they are integrated into the operational process and that they are effective.

All employees, external parties and other stakeholders are required to support the continuous improvement of information security. Employees are encouraged to report potential improvements or vulnerabilities.

Ongoing review of policies and monitoring of their content will ensure the desired level of security and privacy. Discrepancies are analyzed with the aim of improving the information security situation.

Requirements for Suppliers

Information for Classification

All Information, which is transmitted through the suppliers and provided by syracom, are to be handled based on its confidentiality.

Syracom's business requirements for sharing and restricting access to information, as well as regulatory requirements, are addressed through classification and related security measures. The assigned confidentiality level is the primary way of classifying the information.

Confidentiality is the prevention of unauthorized disclosure of information and data. Information labeled as "confidential “, must only be available to authorized individuals based on the permitted manner. When classifying information, the following classification lattice is to be used:

Confidentiality Level	Label	Classification Criteria	Access Restriction
Public	Public	The publication of information does not affect syracom	The information is openly available
Internal Usage	Internal	Unauthorized access to the information can cause minimal damage to syracom	The information is accessible to all employees and certain third-party suppliers.
Confidential	Confidential	Unauthorized access to the information can cause significant damage to syracom	The information is intended for a limited group of employees and authorized third parties.
Secret	Secret	Unauthorized access to the information can cause irreparable damage to the business and/or syracom‘s image	The information can only be accessed by certain individuals only

For all information and information processing facilities, there is a requirement to handle, store, and communicate this Information in accordance with the information classification. All personnel with access to classified Information must follow the rules listed below. Upon violations against these controls (e.g. through disclosure to an unauthorized party), reporting in accordance with the reporting process is mandatory. The handling of values is dependent on the type of Information. Syracom differentiates between “Digital Information” (DI), “Analog Information” (AI) and the “spoken word.”

Internal	Confidential	Secret
Labeling (DI, AI)		
Label „Internal" on document's first page	Label each document page as „Confidential"	Label each document page as „Secret"
Saving and Storage (DI, AI)		
Store on O365/Store in the office	Store on O365 with only specific User Groups allowed/ Store in a locked office or locked cabinet	Encrypted storage in O365/Store in a safe
Printing		
Direct Printing	PIN-Print	Personal Printer in one's direct Office
Deletion and Destruction (DI, AI)		
Normal Deletion/ Paper bin in the building	Normal Deletion/ Removal through Container	Destruction of the digital storage medium, deletion of documents from the central and local storage locations, removal from backups/Disposal via container.
Sharing (DI, AI, GW)		
Sharing allowed only with authorized Individuals	Sharing only permitted with authorized personnel/ Externally encrypted (DI)	Sharing permitted after permission by owner is granted and specifically identified individuals/ Always encrypted (DI)

When making Information available, the need-to-know principle applies. Appropriate technical means (e.g. encryption) should be in place to ensure an adequate level of security. Information can be shared through the following digital communication channels:

- E-Mail
- Transferring data via OneDrive, SharePoint
- Transferring data using other Service Providers, such as Dropbox, Google Drive, etc.
- Transfer of E-Mails and Data using Secureshare
- (Teams)-telephone
- Sharing though the use of SMS-Messages

When transferring data, the classification and handling of the Information must be considered.

The following procedures are in place when transferring digital messages:

Protection requirements based on type of information transfer.	Normal (e.g., Public & internal)	High (e.g., Confidential)	Very High (e.g., Secret)
E-Mail	Allowed without restrictions	Allowed only with transport encryption	Allowed only when encrypting the document
Transferring data via OneDrive, SharePoint	Allowed without restrictions	Allowed without restrictions	Allowed only when encrypting the document
Transferring data using other Service Providers, such as Dropbox, Google Drive, etc.	Allowed without restrictions	Prohibited	Prohibited
Transfer of E-Mails and Data using Secureshare	Allowed without restrictions	Allowed without restrictions	Transport Password mandatory
(Teams)-telephone	Allowed without restrictions	Only allowed after verification of Individuals on the call	Only allowed after verification of Individuals on the call
Sharing though the use of SMS-Messages	Allowed without restrictions	Prohibited	Prohibited

If a supplier is granted access to the syracom network or components of the syracom IT infrastructure on a temporary basis or for the duration of the contract to perform its work, the rules, and regulations within syracom shall also apply to the supplier. The responsible person or entity within the supplier who has requested such access must be able to provide clarification. If a remote connection has been established on a temporary basis, that connection must be closed as soon as a service has been successfully performed.

Technical measures (e.g. a registration process) are used to ensure an appropriate level of security when such components are accessed.

To protect the IT infrastructure from disruptions and to ensure the security of the information processed, stored, and transmitted in it, the supplier who has access to the company's IT systems shall be in compliance with the following provisions:

- The unlawful access and/or distribution of copyrighted content is prohibited.
- Also prohibited, is the access and/or distribution of criminally relevant or unethical content.
- The arbitrary downloading of software, such as the installation or use of unauthorized hardware and software, is not permitted by the supplier or other contractors.
- Access to the Internet or networks not operated by the Company is available only through access points provided by the Company specifically for that purpose.
- Login credentials for use of the IT infrastructure (e.g., passwords) should be kept secret by suppliers and any contractors and should not be shared with third parties. Even within the supplier's or contractor's own organization, the party must keep this information secret from other employees. Exceptions may be made if the contractor's services are provided for syracom by a team of individuals.
- All suppliers and contractors are prohibited from using syracom IT systems for personal use.
- Suppliers are not permitted to process personal data for their own purposes or to process sensitive syracom information for their own purposes to which a supplier has access by virtue of their duties.

Reporting Information Security Incidents

Supplier shall promptly report all Information Security-related events by emailing the following address, Informationssicherheit@syracom.de. The focus here should be on syracom AG Information. If the loss of Confidentiality, Integrity, and Availability of syracom Information is at risk, it must be reported.

The following information must be included in the notification:

- What occurred?
- When did it occur, when was it noticed?
- Who was involved? (Were any third parties involved when the incident was triggered, such as project members?)
- Who is affected by the incident? (syracom employees, applicants, clients, partners? How many people are estimated to be affected?)
- Were measures already taken?

Definitions

Information Security Events, such as Information Security Incidents are defined in the following way:

- **Information Security Event**: Recognized occurrence of a condition of a system, service, or network that indicates a possible violation of the Information Security Policy, the ineffectiveness of measures, or a previously unknown situation that may be security related.

- **Information Security Incident**: Singular and unwanted or unexpected information security event that has a significant probability of compromising the ability of the organization to function and compromises the organization's information security.

Information Security – Incident Management

Upon reporting an Incident, the reported event will first be directed and reviewed by syracom AG's ISB to determine if a potential Incident is occurring or has occurred. In addition, there will be an evaluation of the party responsible for the incident. If no potential incident has occurred, the submitter is notified, and further work is stopped.

Once a potential Information Security Incident has been identified, an explanation of the situation and documentation of any further steps should be undertaken and led by the ISB. The purpose of this situation clarification is to confirm or refute the occurrence of such an incident and to determine the severity of the incident. For this purpose, the ISB and ISB support can call on support from all necessary areas, as well as from the person who reported the incident originally. The following three outcomes and their criteria can be a result of such analysis:

<u>No Relevance identified</u>

- Information Security Incident can be ruled out
- Incident is already fully explained and there is no recognizable damage

<u>Incident identified</u>

- Suspicion of minimal to medium Impact / Damage
- No suspicion of intentional action

<u>Significant Incident identified</u>

- Suspicion of very high Impact / Damage
- Suspicion of an intentional act with minor Impact / Damage

In addition, it should be determined if personal Data was affected. Should this occur, the Data Protection Officer should be included as well.

Example Notifications (Excerpt)

- Accidental sending of an E-Mail with confidential Information to a wrong recipient
- Loss of a syracom end-device (where applicable)
- Loss of the physical Access Card (where applicable)