

Leaflet on Information Protection – Basics

Confidentiality

All SCHOTT employees are obliged to comply with the measures for protecting SCHOTT information in their areas of responsibility and to maintain confidentiality regarding all operational processes – even after termination of employment.

Classification of Information

Classify SCHOTT information according to the classification levels (Public / Internal / Confidential).

IT and communication systems

Always use the IT and communication systems provided to you in a responsible manner. Security settings must not be circumvented or changed.

Authorization management (need-to-know)

Access to SCHOTT information may only be granted if it is necessary for the performance of work tasks (need-to-know principle). Ensure that unauthorized people are prevented from viewing or accessing SCHOTT information and third-party information.

Third parties

Inform third parties, such as temporary workers, suppliers, customers, service providers, or consultants, about the protective measures for SCHOTT information. Check whether a specific confidentiality agreement is necessary.

Communication

The exchange of SCHOTT information must be objectively justified, regardless of the classification level. Assess the risk of information loss and use appropriate protective measures in accordance with the selected classification level.

The use of M365 applications such as Teams, SharePoint, and OneDrive is permitted for information up to the classification level "Confidential."

Mobile working

When working remotely or traveling on business, only carry the information and IT devices you need. Protect them from unauthorized access and do not leave them unattended.

Awareness & Social Engineering

Always be careful when disclosing SCHOTT information. Question the legitimacy or information requests of (unknown) people.

Use of artificial intelligence (AI)

Open-source AI solutions (e.g., ChatGPT; DeepSeek) may not be used for SCHOTT information or personal data. ChatGPT Enterprise or Copilot in Edge are permitted.

Incidents

Report incidents (e.g., loss of information) to Compliance & Security immediately!
Report the loss of IT devices to your IT department immediately!

Further information on information protection can be found in the Information Protection Policy. If you have any questions, please contact Compliance & Security.



Merkblatt Infoschutz – Basics

Verschwiegenheitspflicht

Alle SCHOTT Mitarbeiter*innen sind verpflichtet, die Maßnahmen zum Schutz von SCHOTT Informationen in ihren Verantwortungsbereichen einzuhalten sowie Verschwiegenheit über alle betrieblichen Vorgänge zu wahren – auch nach Beendigung des Arbeitsverhältnisses.

Klassifizierung von Informationen

Klassifizieren Sie SCHOTT Informationen gemäß den Klassifizierungsstufen (Public / Internal / Confidential).

IT- und Kommunikationssysteme

Gehen Sie stets verantwortungsbewusst mit Ihnen zur Verfügung gestellten IT- und Kommunikationssystemen um. Sicherheitseinstellungen dürfen nicht umgangen oder geändert werden.

Berechtigungsmanagement (Need-to-know)

Der Zugriff auf SCHOTT Informationen darf nur dann ermöglicht werden, wenn dieser zur Erfüllung der Arbeitsaufgabe notwendig ist (Need-to-Know-Prinzip). Achten Sie darauf, dass der Einblick oder Zugriff unberechtigter Personen auf SCHOTT Informationen und Informationen Dritter verhindert wird.

Dritte

Weisen Sie Dritte, beispielsweise Leiharbeiter, Lieferanten, Kunden, Dienstleister oder Berater, auf die Schutzmaßnahmen für SCHOTT Informationen hin. Prüfen Sie die Notwendigkeit einer spezifischen Geheimhaltungsvereinbarung.

Kommunikation

Der Austausch von SCHOTT Informationen muss unabhängig von der Klassifizierungsstufe objektiv gerechtfertigt sein. Prüfen Sie das Risiko eines Informationsverlustes und verwenden Sie gemäß der gewählten Klassifizierungsstufe entsprechende Schutzmaßnahmen.

Die Nutzung von M365 Applikationen wie Teams, SharePoint und OneDrive ist für Informationen bis zur Klassifizierungsstufe „Confidential“ erlaubt.

Mobiles Arbeiten

Führen Sie beim mobilen Arbeiten oder auf Geschäftsreisen nur die dafür benötigten Informationen und IT-Geräte mit sich. Schützen Sie diese vor ungewolltem Zugriff und lassen Sie sie nicht unbeaufsichtigt.

Awareness & Social Engineering

Seien Sie bei der Preisgabe von SCHOTT Informationen stets vorsichtig. Hinterfragen Sie die Legitimation bzw. das Informationsanliegen von (unbekannten) Personen.

Einsatz von Künstlicher Intelligenz (KI)

Open-Source-KI-Lösungen (z.B. ChatGPT; DeepSeek) dürfen für SCHOTT Informationen oder personenbezogene Daten nicht verwendet werden. Zulässig sind ChatGPT Enterprise oder der Copilot in Edge.

Vorkommnisse

Melden Sie Vorkommnisse (z.B. den Verlust von Informationen) sofort an Compliance & Security!
Melden Sie den Verlust von IT-Geräten umgehend Ihrer IT!

Weiterführende Hinweise zum Informationsschutz finden Sie in der Informationsschutz-Richtlinie. Bei Fragen können Sie sich gerne an Compliance & Security wenden.

