

Informationssicherheit

Um die Informationssicherheit in einer Organisation strukturiert zu implementieren, wird ein Informationssicherheitsmanagementsystem (ISMS) benötigt. Dabei geht es vorrangig um die Systematik, wie ein ISMS aufzubauen und was dabei zu beachten ist. Es handelt sich hierbei nicht um ein „fertiges“ System oder Produkt, das alles (teil-)automatisiert erledigt, sondern um einen Prozess.

Ein ISMS übernimmt demnach Planungs-, Lenkungs- und Kontrollaufgaben, die erforderlich sind, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen bzw. zu verbessern.

Die Hochschule Trier beabsichtigt in den kommenden Jahren ein ISMS zu etablieren.

*Fabian Amon
Informationssicherheitsbeauftragter (ISB)
der Hochschule Trier*

Clean Desk Prinzip

Um Angreifern den Weg an Ihre Daten zu erschweren, sollten möglichst wenige bzw. keine (analoge und digitale) Informationen beim Verlassen des Büros einsehbar sein. Dieser Artikel über das Clean Desk Prinzip beschreibt anhand von Beispielen, wie Ihnen dies einfacher gelingt und was Sie dabei beachten müssen.

Dokumentenmanagement>>>

Achten Sie darauf, dass sensiblen Dokumente, Datenträger, USB-Sticks, o. Ä. nicht öffentlich-zugänglich sind (z. B. auf dem Schreibtisch). Sperren Sie diese immer in Rollcontainern oder Schränken ein (lassen Sie den Schlüssel nicht am Arbeitsplatz liegen). Dokumente, die nicht mehr benötigt werden, entsorgen Sie am besten über den Aktenvernichter, digitale Speichermedien über die Rechenzentren.

Bildschirm Sperre aktivieren>>>

Sperren Sie jedes Mal beim Verlassen des Arbeitsplatzes Ihren PC/Notebook (■ + I). In Büroräumen, die an öffentlich-zugängliche Bereiche, Flure usw. angren-

zen, sollten die Türen immer geschlossen werden. Falls Sie den Arbeitsplatz für mehr als 5 Minuten verlassen, sperren Sie stets die Bürotür ab. Speichern Sie ebenfalls alle Dateien ab, sodass beim unerwarteten Herunterfahren oder Absturz die Informationen auch nach einem Neustart weiterhin zur Verfügung stehen.

Mobile Arbeit>>>

Bei der Informationssicherheit und dem Datenschutz gilt der Grundsatz der Datenminimierung. Nehmen Sie nur so viel Daten mit nach Hause, wie nötig. Versuchen Sie möglichst digital zu arbeiten und so wenig wie möglich auszudrucken (vermeiden von Duplikaten). Dies hilft nicht nur der Informationssicherheit, sondern auch unserer Umwelt.



Verschluss sachen>>>

Als Hochschule bewegen wir uns im Spannungsfeld zwischen akademischer Offenheit und dem Schutz sensibler Informationen. Ob innovative Forschungsergebnisse, Prüfungsunterlagen oder geschützte Personaldaten – bestimmte Informationen erfordern durch ihren Einstufungsstatus als Verschluss sache (VS) ein besonders hohes Maß an Vertraulichkeit. Grundsätzlich wird zwischen den folgenden unterschieden:

VS – Nur für den Dienstgebrauch (intern), VS – Vertraulich.

Geheim und Streng geheim fallen derzeit auch unter vertraulich.

Weitere wichtige Informationen erhalten Sie in der Richtlinie zur Lenkung von Dokumenten und [BSI_CON.11.1](#)



Notfallkontakt bei IT-Vorfällen

Bei **Informationssicherheitsvorfällen** wenden Sie sich umgehend telefonisch an die: +49 651 8103-777 oder per E-Mail an: informationssicherheit@hochschule-trier.de