



Dokumentation für Geheimnisträger

Informationsschutz

1 Die nachrichtendienstliche Bedrohung

Heutzutage ist nicht immer klar ersichtlich, wo Gefahren lauern. Aufgrund der Komplexität und Vernetzung der Abläufe sind nicht nur klassische militärische Informationen Ziele von Spionage. Auch Bereiche der Wirtschaft wie Industrie, Banken und die Verwaltung mit ihren öffentlichen Diensten sind ins Fadenkreuz fremder Staaten, Konkurrenten und weiterer Organisationen gerückt. Demokratien mit ihren offenen Gesellschaftsformen sind besonders anfällig gegen Spionage, Sabotage und Terroroperationen.

Spioniert und ausgeforscht wird überall und jederzeit!

Das Spionieren und Sammeln von Informationen wird überdies durch die globale Vernetzung der Informatik- und Telekommunikationssysteme, die hohe Übertragungskapazität und den zunehmenden Drang zur Offenlegung möglichst vieler Informationen massiv erleichtert. Auch Freunde werden ausspioniert.

2 Zweck des Informationsschutzes

Mit Informationsschutz- und Sicherheitsmassnahmen soll verhindert werden, dass Unbefugte, fremde Nachrichtendienste oder die Öffentlichkeit von schutzwürdigen Informationen Kenntnis erhalten. Es geht konkret darum, die illegale Beschaffung nachrichtendienstlich interessanter Informationen aus sensiblen Bereichen von Wirtschaft, Verwaltung, Armee und Industrie zu verunmöglichen.

Informationen

Unter den Begriff Informationen fallen Aufzeichnungen aller Art, namentlich in Schrift, Bild und/oder Ton, in elektronischer Form (*Informatik*) sowie mündliche Äusserungen.

Schutzwürdige Informationen sind entsprechend ihrer Bedeutung zu kennzeichnen:

GEHEIM	Informationen, deren Kenntnisnahme durch Unberechtigte den Landesinteressen einen schweren Schaden zufügen kann.
VERTRAULICH	Informationen, deren Kenntnisnahme durch Unberechtigte den Landesinteressen Schaden zufügen kann.
INTERN	Informationen, deren Kenntnisnahme durch Unberechtigte den Landesinteressen einen Nachteil zufügen kann; und die weder als GEHEIM noch als VERTRAULICH klassifiziert werden müssen.

3 Pflichten der Mitarbeitenden

3.1 Pflicht zur Geheimhaltung

Die Pflicht zur Geheimhaltung schutzwürdiger Informationen ergibt sich aus dem Militärstrafgesetz, dem Strafgesetzbuch, dem Bundespersonalgesetz und - für Angehörige der Armee - aus dem Dienstreglement. Das Bundespersonal hat auch nach Inkrafttreten des Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung in vielen Fällen das Amts-geheimnis zu wahren.

Die Verpflichtung zur Verschwiegenheit gilt für alle schutzwürdigen Informationen, die in amtlicher oder dienstlicher Funktion erstellt oder zur Kenntnis genommen werden, auch wenn sie nicht klassifiziert sind.

Die Geheimhaltungspflicht gilt auch nach Beendigung des Dienst- bzw. Arbeitsverhältnisses.

3.2 Allgemeine Schutzmassnahmen

Schutzwürdige Informationen dürfen nur berechtigten Personen zur Kenntnis gebracht werden.

Es gilt das Prinzip:

KENNTNIS NUR WENN NÖTIG !

Die Merkmale der Geheimhaltung sind:

SCHWEIGEN	Auskünfte über schutzwürdige Informationen ausschliesslich Berechtigten gewähren.
EINSCHLIESSEN	Schutzwürdige Informationen und Material unter Verschluss halten.
TARNEN	... wenn SCHWEIGEN und/oder EINSCHLIESSEN nicht ausreichen oder nicht möglich sind.

3.3 Konkrete Schutzmassnahmen

a) am Arbeitsplatz:

- Lassen Sie klassifizierte Informationen nicht unbeaufsichtigt an Ihrem Arbeitsplatz liegen; schliessen Sie diese ein, wenn Sie Ihren Arbeitsplatz verlassen (*Clean Desk Policy*). Denken Sie daran, dass Informationsträger mit GEHEIMEN, VERTRAULICH und INTERN klassifizierten Informationen korrekt (*gemäss Weisungen über die detaillierten Bearbeitungsvorschriften zum Informationsschutz*) aufbewahrt werden müssen.
- Sperren Sie beim Verlassen des Büros immer den PC.
(*Smartcard entfernen oder Windows- und "L"-Taste gleichzeitig drücken*).
- Vergessen Sie nicht, auch alle Schlüssel sicher aufzubewahren; entweder im persönlichen Gewahrsam oder in einem Behältnis mit Sicherheits- oder Codeschloss.
- Werfen Sie kein Zwischenmaterial (*Entwürfe, Notizen, Skizzen, elektronische Informationsträger jeglicher Art, usw.*) in den Papierkorb, sondern vernichten Sie es gemäss den einschlägigen Weisungen und Vorschriften. Halten Sie sich im Übrigen an die Anweisungen Ihres Arbeitgebers über die Bearbeitung von klassifizierten Informationen.
- Entstehen irgendwelche Zweifel oder Unklarheiten über Klassifizierung, Schutzwürdigkeit sowie Sicherheit, wenden Sie sich an Ihren Chef Sicherheit oder den Informationsschutz- bzw. Geheimschutzbeauftragten.

b) gegenüber Drittpersonen:

- Bewahren Sie Verschwiegenheit über alle Ihnen mündlich oder schriftlich zur Kenntnis gelangenden Angelegenheiten, die Ihnen gegenüber als klassifiziert bezeichnet worden sind oder deren Schutzwürdigkeit sich aus ihrem Inhalt ergibt.
- Seien Sie vorsichtig bei Gesprächen über klassifizierte Informationen und achten Sie darauf, dass kein Unbefugter das Gespräch mithören kann. Überzeugen Sie sich stets davon, ob die Gesprächspartner Kenntnis erhalten dürfen und im erforderlichen Umfang zu klassifizierten Informationen zugangsberechtigt sind. Geben Sie Ihrem Gesprächspartner mit aller Deutlichkeit zu erkennen, welche Angelegenheiten klassifiziert sind und damit der Geheimhaltungspflicht unterliegen.
- Vermeiden Sie Gespräche mit klassifiziertem Inhalt in der Öffentlichkeit oder in ungesicherten Räumen (*Hotelzimmer, Restaurant, öffentliche Verkehrsmittel, usw.*).

- Achten Sie darauf, sich bei Gesprächen mit Unbekannten nicht durch falsche Behauptungen oder vorgetäuschte Sachkenntnis zum Ausplaudern von Geheimnissen verleiten zu lassen.
- Unbekannten Personen dürfen Sie keine persönlichen Ausweisschriften, Aufenthaltsbewilligungen, Mitgliedsausweise, Zutrittsbadges, Schlüssel, Passfotos, usw. überlassen. Auch nicht für kurze Zeit!
- Berücksichtigen Sie, dass Telekommunikationsverbindungen in den seltensten Fällen sicher sind. Namentlich beim Gebrauch des Internets und den mobilen Kommunikationsgeräten hinterlassen Sie Spuren, die weltweit eingesehen und nachverfolgt werden können.
- Eine E-Mail ist mindestens so öffentlich wie eine Ansichts- oder Postkarte. Klassifizierte Informationen müssen vor dem Versand mit einer von der IOS zugelassenen Software verschlüsselt werden.
- Klassifizierte Dokumente dürfen per Fax nur mit den von der Führungsunterstützungsbasis (*FUB/ISA, Krypt*) zugelassenen Geräten übermittelt werden.

4 Auskünfte/Meldungen

Für Fragen im Zusammenhang mit der Integralen Sicherheit wenden Sie sich bitte an die für Ihren Bereich zuständigen Personen:

Armee	Verwaltung	Industrie
C FGG 6 in den Stäben und Armeestabteilen der DU CdA sowie den Stäben der Grossen Verbände.	Chef Integrale Sicherheit oder Informationsschutz- bzw. Informatiksicherheitsbeauftragte der Verwaltungseinheit.	Geheimschutzbeauftragter der Firma.
oder direkt an: Generalsekretariat VBS / IOS Informationssicherheit Papiermühlestrasse 20 CH-3003 Bern Tf. Nr. 058 463 38 48 / Fax Nr. 058 463 38 41		

Verdächtige Umtriebe oder ein Spionageverdacht können gemeldet werden:

- im Zivilleben direkt dem Nachrichtendienst des Bundes, CH-3003 Bern, Tel. 058 462 45 11
- während des Truppendienstes der Militärische Sicherheit, Tel. 0800 55 23 33 oder gemäss Reglement 51.024 d Organisation der Ausbildungsdienste (*ODA*).
- innerhalb des VBS ist in jedem Fall eine Sicherheitsmeldung gemäss SIME-Weisungen zu erstatten.

5 Konsequenzen bei Verletzung der Geheimhaltungspflicht

Jede Verletzung der Geheimhaltungspflicht kann den Interessen unseres Landes und damit der Allgemeinheit Schaden zufügen. Leidtragende können letztlich Ihre Angehörigen, Ihr Arbeitgeber und/oder Sie selbst sein. Für Sie persönlich kann eine Verletzung der Geheimhaltungspflicht überdies disziplinarische, straf- und/oder zivilrechtliche Folgen nach sich ziehen.

Die Einhaltung der oben aufgezeigten Regeln stellt den Schutz unserer wichtigsten Informationen sicher und schützt Sie vor Konflikten mit dem Gesetz. Der Aufwand für Sie ist im Verhältnis zu den möglichen Konsequenzen klein. Wir danken Ihnen für die konsequente Einhaltung und Umsetzung der Vorschriften!

Bern, 1. Juli 2016

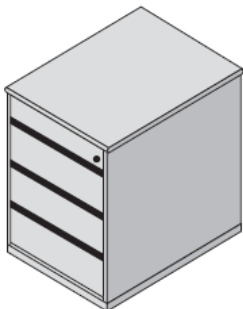
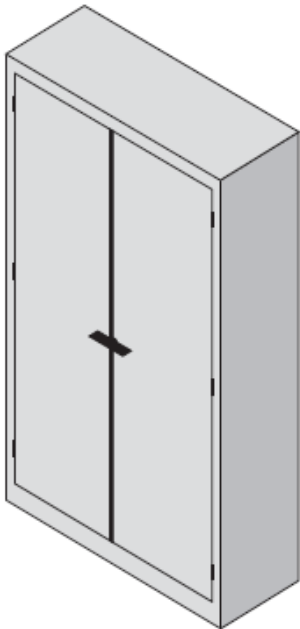
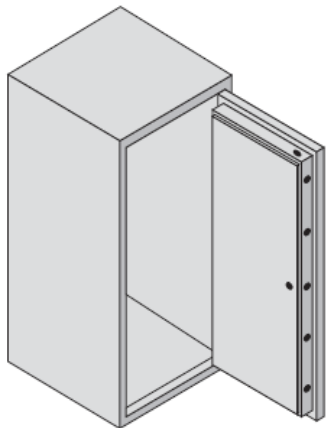
Generalsekretariat VBS
Informations- und Objektsicherheit IOS

Verteiler

- alle Mitarbeitenden des VBS
- Stäbe und Einheiten der Armee
- Mitarbeitende von Firmen im Geheimschutzverfahren
- Internet IOS (*Publikation*)

... zur Erinnerung !

Für die **Aufbewahrung von klassifizierten Informationen** gelten, gemäss Informationsschutzvorschriften vom 1. Januar 2015 (*Dokumentation 52.064*), folgende Vorschriften:

INTERN	VERTRAULICH	GEHEIM
Unter Verschluss	Sicherheitsbehältnis	Tresor
	Wird von der IOS/INS abgenommen.	VdS-Klasse III (Widerstandsklasse 3)
		
Symbolbilder !		

Siehe auch:

Weisungen über die detaillierten Bearbeitungsvorschriften zum Informationsschutz (*Bearbeitungsweisungen*) vom 18. Januar 2008

