Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Bundesamt für Sport BASPO
Sportpolitik und Ressourcen

Paolo Dünner, 19.10.2020 **Öffentlich**

Information-Sicherheit-Management-System (ISMS) BASPO

Melden von Sicherheitsvorfällen

Dokumentenkontrolle	
Gültig von / bis	19.10.2020
Version	2.0
Status	Freigegeben
Dokumenten-Art	Merkblatt
Verteiler	
Dok.-Eigner	Häusler Roland BASPO
Geltungsbereich	BASPO
Ablageort	GRCS

Prüfung

Name	Rolle	Datum / Version
Cyril Stauffer	ISBO	08.10.2018
Fritz Amsler	ISBO	05.10.2020

Freigabe

Name	Rolle	Datum / Version
Roland Häusler	Leiter IT BASPO	09.10.2018
Roland Häusler	Leiter IT BASPO	19.10.2020

Inhaltsverzeichnis

1 Einführung

1.1 Ziel und Zweck

Das vorliegende Dokument soll Mitarbeitenden, Linienvorgesetzten, Service Desk und anderen Personen aufzeigen, welche Ereignisse als Sicherheitsvorfälle gelten und gemeldet werden müssen.
Sicherheitsvorfälle können versehentlich oder absichtlich geschehen. Sie können Personen, Gebäude, Systeme oder Informationen betreffen. Auch sogenannte Beinahe-Sicherheitsvorfälle, also solche, die zu einem Sicherheitsvorfall hätten führen können, sind zu melden.

2 Zu meldende Sicherheitsvorfälle

Der Mitarbeitende meldet einen Sicherheitsvorfall seinem Linienvorgesetzten oder falls dringend dem ISBO oder dem C Sich (mit nachträglicher Information des Linienvorgesetzten) per

- Telefon (ISBO; C Sich; Linienvorgesetzten; gemäss Intranet „Sicherheit am BASPO“),
- Email (sicherheit@baspo.admin.ch)

Die folgende Liste enthält Beispiele sicherheitsrelevanter Vorfälle und Schwachstellen (nicht abschliessend), die es umgehend zu melden gilt:

1. Absichtliche Beschädigung oder Diebstahl von **IT-Ausrüstung** oder -Geräten
2. Infizierung mit schädigender oder störender Software (z. B. Malware wie **Viren**, Computerwürmer, Trojaner)
3. Verlust, Diebstahl oder unberechtigte Vernichtung von vertraulichen **Informationen** oder schützenswerten **Personendaten**
4. Vertrauliche Informationen oder schützenswerte Personendaten, die auf **öffentlichen Plattformen** gespeichert sind (z. B. dropbox.com)
5. Aus Versehen wurden **medizinische Daten** von Athleten veröffentlicht
6. Bei der **Entsorgung** von Datenträgern wurden diese Dritten zugänglich gemacht, die darauf besonders schützenswerte Personendaten einsehen konnten
7. Ein **Datenschutzverstoss** gelangt an die Öffentlichkeit, es ist mit Mitteilungen in der Presse zu rechnen
8. Mündlich oder schriftlich geäusserte **Drohungen** gegenüber Kunden oder Mitarbeitende
9. Nicht eindeutig identifizierbare oder **unbefugte** Personen halten sich in gesicherten Bereichen (z.B. Sicherheitszone) auf
10. Mitarbeiter werden durch unbefugte Personen gezielt über vertrauliche Informationen befragt, wie zu Passwörtern oder technischer Infrastruktur (**Social Engineering**)
11. Missbrauch oder Blockierung von Systemressourcen, **IT-Systemen**
12. Unerklärbare Sperrung von **Zugangsdaten**
13. Fehlende oder **unwirksame Sicherheitskontrollen** (z. B. ungewohntes Login ohne Passwortaufforderung)
14. **Verstoss** gegen Richtlinien, Weisungen oder Sicherheitsvorschriften
15. Aufgebrochene **Türen oder Fenster**
16. gravierende **Funktionsfehler** bei Software oder Hardware
17. Entdeckung vertraulicher Informationen oder schützenswerter Personendaten bei der Benutzung öffentlicher **Suchmaschinen** (z. B. Google)
18. **Website**-Defacement (z. B. Aussehen einer bekannten Website erscheint verändert oder verdächtig, oder Inhalt ist schlecht übersetzt)