1. Sicherheits- und Datenschutzvorfälle

Alle sicherheits- oder datenschutzrelevanten Ereignisse sowie erkannte Schwachstellen, die Auswirkungen auf die SVD Büromanagement GmbH (kurz: „SVD“) haben, sind sofort dem Informationssicherheitsbeauftragten der SVD zu melden (siehe Kapitel 7 „**Fehler! Verweisquelle konnte nicht gefunden werden.**“). Für die Aufklärung der Ereignisse sind sämtliche für die Aufklärung notwendigen und hilfreichen Informationen bereitzustellen.

Beispiele für sicherheits- oder datenschutzrelevante Ereignisse sind

- Verdacht auf Missbrauch von Benutzerkennungen,
- ungewünschte Veröffentlichung von internen Daten der SVD im Internet,
- Verlust / Diebstahl von IT-Systemen oder Datenträgern mit internen Daten der SVD,
- versehentliches Versenden eines E-Mails mit internen Daten der SVD an den falschen Empfänger,
- Infektion mit Schadsoftware
- etc.

2. Fernwartungszugriff

Wird dem Externen im Zuge seiner Tätigkeit für die SVD ein Fernwartungszugriff auf Systeme der SVD zur Verfügung gestellt, sind die folgenden Vorgaben einzuhalten:

- Der Fernwartungszugang darf ausschließlich von denjenigen Personen verwendet werden, für die der Zugang zur Verfügung gestellt wurde.
- Der Fernwartungszugang darf nur für dienstliche Zwecke und ausschließlich zur Durchführung der vereinbarten Tätigkeiten verwendet werden. Jede andere Verwendung ist ausdrücklich untersagt.
- Eine geöffnete Fernwartungssitzung darf nicht unbeaufsichtigt gelassen werden.
- Sobald die durchzuführenden Tätigkeiten erledigt sind und die Fernwartungssitzung nicht mehr benötigt wird, ist diese umgehend zu schließen.
- Der Externe hat Aufzeichnungen über die durchgeführten Tätigkeiten zu führen und diese auf Anfrage an die SVD zu übermitteln. Die Aufzeichnungen haben mindestens folgendes zu enthalten:
    - Mitarbeiter, der eine Tätigkeit durchgeführt hat
    - System, auf dem die Tätigkeit durchgeführt wurde
    - Beschreibung der durchgeführten Tätigkeit
    - Startzeitpunkt der durchgeführten Tätigkeit (Datum und Uhrzeit)
    - Endzeitpunkt der durchgeführten Tätigkeit (Datum und Uhrzeit)
- Alle Fernwartungszugriffe sowie auf den Systemen der SVD durchgeführten Tätigkeiten werden protokolliert und ggf. ausgewertet.
- Der Externe hat dem aktuellen Stand der Technik entsprechende technische und organisatorische Maßnahmen umzusetzen, um sicherzustellen, dass die Fernwartungsverbindung nicht missbräuchlich verwendet wird und kein unbefugter Zugriff auf Daten und Systeme der SVD besteht.
- Bei Verdacht auf Missbrauch des Fernwartungszugangs ist dies unverzüglich dem Informationssicherheitsbeauftragten der SVD zu melden.

3. Fotografieren und Filmen

Das Fotografieren und Filmen in den Räumlichkeiten der SVD – im Speziellen im Rechenzentrum der SVD – ist untersagt.

4. Technische und organisatorische Maßnahmen (TOMs)

Der Externe hat in seinem Verantwortungsbereich dem aktuellen Stand der Technik entsprechende technische und organisatorische Maßnahmen umzusetzen, um sicherzustellen, dass die Daten der SVD angemessen vor unbefugtem Zugriff, Veröffentlichung, Zerstörung und Manipulation geschützt sind. Dazu zählen insbesondere die in den folgenden Kapiteln beschriebenen Maßnahmen.

4.1 Verschlüsselung von externen Speichermedien

Werden Daten der SVD auf externen Speichermedien (z.B. USB-Sticks) gespeichert, so sind diese gemäß dem aktuellen Stand der Technik zu verschlüsseln. Als Passwort ist ein sicheres Passwort gemäß den Vorgaben in Kapitel 4.7 zu wählen.

4.2 Absicherung der E-Mail-Kommunikation

Um eine Sicherung von E-Mails auf dem Transportweg zu gewährleisten, ist die Verschlüsselung des Transportwegs (zumindest Server zu Server) auf den Mailservern des Externen zu aktivieren.

4.3 Übertragung von personenbezogenen Daten

Personenbezogene Daten (z.B. in Datenbank-Dumps, Backups, Screenshots mit derartigen Daten usw.) dürfen **nicht unverschlüsselt per E-Mail übertragen** werden! Es ist ein sicherer Übertragungsweg zu verwenden (z.B. Transportverschlüsselung der E-Mail-Kommunikation, Ende-zu-Ende-Verschlüsselung der E-Mail-Kommunikation, verschlüsselte ZIP-Datei, Private-Cloud-Lösung etc.).

4.4 Verschlüsselung von mobilen IT-Systemen

Alle mobilen IT-Systeme (z.B. Notebooks, Smartphones etc.), mit denen Zugriff auf Daten oder Systeme der SVD möglich ist, müssen über eine Festplattenverschlüsselung bzw. Datenspeicherverschlüsselung verfügen.

4.5 Virenschutz

Alle Systeme, mit denen Zugriff auf Daten oder Systeme der SVD möglich ist bzw. auf denen Daten der SVD gespeichert sind, sind mit einer Virenschutzlösung vor Schadsoftware zu schützen. Die Virendefinitionen sind regelmäßig (mehrmals täglich) zu aktualisieren.

4.6 Patch Management

Auf allen Systemen, mit denen Zugriff auf Daten oder Systeme der SVD möglich ist bzw. auf denen Daten der SVD gespeichert sind, sind sicherheitsrelevante Patches zeitnah zu installieren. Dies betrifft nicht nur Patches des Betriebssystems selbst, sondern auch von zusätzlich installierten Applikationen. Es dürfen nur Betriebssysteme verwendet werden, die vom Hersteller mit sicherheitsrelevanten Patches versorgt werden.

4.7 Passwörter

Alle Zugänge, mit denen Zugriff auf Daten oder Systeme der SVD möglich ist, sind mit einem personalisierten Passwort vor unbefugtem Zugriff zu schützen. Bei der Wahl des Passworts sind folgende Vorgaben einzuhalten:

- Länge: mind. 12 Zeichen
- Komplexität (Verwendung von Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen)

- Vermeidung von Personennamen (z. B. eigener Name, Name des Partners, Namen der Kinder, Name des Haustiers)
- Vermeidung von Systemnamen (z. B. Kennung des eigenen Arbeitsgeräts)
- Vermeidung von allen Wörtern, die in einem Wörterbuch vorkommen (auch fremdsprachige Wörterbücher)
- Vermeidung einfacher Buchstaben- und Zahlenkombinationen (z. B. abcdef, 1234 usw.)
- Trennung der Kennwörter für Firmen- und Privatgebrauch
- Sonderzeichen und Zahlen sollten nicht am Schluss an das Passwort angehängt werden
- Ablauf nach 365 Tage

Jeder Mitarbeiter des Externen ist für die sichere Auswahl des Passworts und dessen Geheimhaltung verantwortlich. Die Weitergabe des persönlichen Benutzereinstiegs ist nicht zulässig.

Passwörter können auf freiwilliger Basis jederzeit geändert werden. Bei Verdacht auf Kompromittierung sind Passwörter zwingend zu ändern. Initialpasswörter sind bei der ersten Anmeldung auf persönliche Passwörter zu ändern.

4.8 Personalisierte Zugänge

Alle Zugänge, mit denen Zugriff auf Daten oder Systeme der SVD möglich ist, müssen personalisiert sein. Der Zugriff auf Daten mittels Gruppenuser ist zu unterbinden. Es muss zu jedem Zeitpunkt nachvollziehbar sein, welcher Benutzer auf welche Daten oder Systeme der SVD zugegriffen hat.

4.9 Clear Desk / Clear Screen

Alle Daten der SVD (digital oder ausgedruckt) sind vor unbefugtem Zugriff zu schützen.

Ausgedruckte Dokumente dürfen nicht offen liegen gelassen werden. Ausgedruckte Dokumente dürfen nicht im Drucker verbleiben, sondern sind ehestmöglich abzuholen. Das gilt insbesondere für Räumlichkeiten, zu denen auch Externe Zugang haben. Nicht mehr benötigte vertrauliche Dokumente sind sicher zu vernichten (z.B. mittels geeignetem Aktenvernichter). Zudem ist darauf zu achten, dass das Führen von vertraulichen Telefonaten / Gesprächen, die die SVD betreffen, nur in einer leicht zu überblickenden Umgebung stattfinden soll.

Alle Clients, mit denen Zugriff auf Daten oder Systeme der SVD möglich ist, sind bei Abwesenheit zu sperren.

4.10 Vernichtung von Daten

Ausgeschiedene Datenträger sowie nicht mehr benötigte Dokumente, auf denen Daten der SVD enthalten sind, sind sicher zu vernichten.

5. Auditrecht

Die SVD hat das Recht, die Einhaltung der Sicherheitsmaßnahmen beim Externen zu überprüfen oder durch einen beauftragten Dritten überprüfen zu lassen.

6. Informations- und Rückgabepflicht bei Personaländerungen

Tritt ein Mitarbeiter des Externen aus dem Unternehmen aus bzw. ändert sich sein Aufgabengebiet, sodass er keine Tätigkeiten mehr für die SVD durchführt, hat der Externe die SVD rechtzeitig darüber

zu informieren. An den Mitarbeiter ausgegebene Geräte oder Zutrittskarten der SVD sind an die SVD zurückzugeben.

7. Kontaktdaten

	Rolle	Telefon
	Informationssicherheitsbeauftragter	+43 (0) 1 / 798 14 14 – 233
	Datenschutzmanager	+43 (0) 1 / 798 14 14 – 231