Erfassung Sicherheitsvorfall

Hitz - Treuhand GmbH
Andrea Hitz
Sonnenbühlstrasse 14
8181 Höri
Schweiz

Version 1.1, 05.09.2024

Maßnahmen und Meldeprozess

1. Information des Verantwortlichen (Inhaber, Geschäftsführer)
2. Information des Datenschutzbeauftragten
3. Information des IT-Verantwortlichen
4. Ausfüllen des Erfassungsbogen
    1. Bewertung des Vorfalls
    2. Einstufung der Gefährdungslage (Geschäftsführung, Datenschutzbeauftragter und IT-Verantwortlicher)
5. Meldung an die zuständige Datenschutzbehörde durch den Verantwortlichen durch das Ausfüllen der Online Meldung

1. Kontaktdaten der Zuständigen Datenschutzbehörde

Online-Service

Für die Meldung steht ein Online Service unter: https://databreach.edoeb.admin.ch/report zur Verfügung.

Schweiz
Aufsichtsbehörde

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

Anschrift:	Feldeggweg 1 CH - 3003 Bern
Telefon:	+41 (0)58 462 43 95 (Mo. bis Fr., 10.00 bis 12.00 Uhr)
Telefax:	+41 (0)58 465 99 96
Internet:	https://www.edoeb.admin.ch/edoeb/de/home/deredoeb/kontakt.html

2. Erfassung von IT-Sicherheitsvorfällen

Angaben zum IT-Sicherheitsvorfall

Datum und Uhrzeit:	
ID des IT-Sicherheitsvorfalls:	
ID ähnlich gelagerter Sicherheitsvorfälle (sofern vorhanden):	

Angaben zum Erfasser des IT-Sicherheitsvorfalls-Reports:

Vor- und Nachname		Anschrift	
Telefonnummer		E-Mail	

Involvierte Mitglieder des Expertenteams

Vor- und Nachname		Anschrift	
Telefonnummer		E-Mail	

Vor- und Nachname		Anschrift	
Telefonnummer		E-Mail	

Beschreibung des IT-Sicherheitsvorfalls

Was ist vorgefallen?

Wie hat sich der Vorfall ereignet?

Welche Ursache hatte der IT-Sicherheitsvorfall?

Welche Systeme / Objekte sind betroffen?

Sind negative Auswirkungen auf Geschäftsprozesse zu erwarten

- Sind Schwachstellen identifiziert worden?

3. Detailinformationen zum IT-Sicherheitsvorfall

Datum und Uhrzeit des Eintritts des IT-Sicherheitsvorfalls (TTMMJJJJ, HHMM)

Datum und Uhrzeit der Erkennung des IT-Sicherheitsvorfalls

Datum und Uhrzeit der Meldung des IT-Sicherheitsvorfalls

Ist der IT-Sicherheitsvorfall abgeschlossen? (Zutreffendes bitte ankreuzen)

□ JA
Wenn JA, wie lange hat der IT-Sicherheitsvorfall angedauert? _____

□ NEIN
Wenn NEIN, wie lange dauert der IT-Sicherheitsvorfall bereits an?_____

4. *Typ des IT-Sicherheitsvorfalls*

(Zutreffendes bitte ankreuzen)

- □ Tatsächlich eingetreten
- □ Versuch
- □ Verdacht
- □ Vorsätzlich
- □ Zufällig

Was ist Gegenstand des Sicherheitsvorfalls?

□	Diebstahl	□	Hacking / Ausspähung von Daten
□	Betrug	□	Sabotage
□	Informationsabfluss	□	Nicht autorisierte Verwendung von Ressourcen
□	Sabotage / Physikalische Beschädigung	□	Anderer Typ Welcher:

□	Hardware Fehler	□	Netzwerk Fehler
□	Software Fehler	□	schädlicher Code
□	Ausfall essentieller Dienste	□	Personalknappheit
□	Feuer	□	Wasser
□	Andere Welche:	□	Andere natürliche Ereignisse Welche:

5. *Fehler (Klassifizierung des Vorfalls)*

□	Systemausfall	□	Fehlbedienung
□	Hardware Wartungsfehler	□	Planungsfehler
□	Software Wartungsfehler	□	Andere, Welche:

□	Unbekannt (Sofern der Sicherheitsvorfall noch nicht klassifiziert werden kann,		

	kreuzen Sie "Unbekannt“ an und beschreiben Sie soweit möglich den Typ des IT-Sicherheitsvorfalls)		

6. Betroffene Gegenstände

Auflistung der vom Sicherheitsvorfall betroffenen Gegenstände (Angabe des Schutzbedarfs, wenn möglich):

Informationen / Daten	
Hardware	
Software	
Kommunikationssysteme	
Dokumente	
IT-Service	
Betroffener Kunde	

7. Auswirkungen des IT-Sicherheitsvorfalls

Sofern zutreffend, kreuzen Sie untenstehende Kategorien an und gewichten Sie die folgenden Auswirkungen auf einer Skala von 1 bis 10.

- Finanzieller Verlust / Störung von Geschäftsprozessen (FG)
- Verlust des Schutzes kommerzieller und wirtschaftlicher Interessen (KW)
- Preisgabe personenbezogener Daten (PD)
- Verstoß gegen gesetzliche und behördliche Verpflichtungen (GB)
- Beeinträchtigung von Management- und Geschäftsprozessen (MG)

		Gewichtung (Skala 1-10)	Auswirkung (Kurzform)	Kosten
□	Verlust der Vertraulichkeit			
□	Verlust der Integrität			
□	Verlust der Verfügbarkeit			
□	Verletzung von Nachweispflichten			
□	Zerstörung			

8. Gesamtkosten für die Bewältigung des IT-Sicherheitsvorfalls

Gewichtung	Auswirkung	Kosten

9. Behandlung des IT-Sicherheitsvorfalls

Datum des Beginns der Behandlung	

Namen der in die Behandlung involvierten Personen	
Datum der Bewältigung des IT-Sicherheitsvorfalls	
Datum des Ende der Auswirkungen durch den Sicherheitsvorfall	
Datum der Beendigung der Ermittlungen	
Verweis und Speicherort des Ermittlungsberichtes	

10. Verursacher

□	Person	□	Organisation / Institution
□	Organisierte Gruppe	□	Zufall
□	Kein Verursacher z.B. natürliche Ereignisse, Ausfall elektronischer Komponenten, menschliche Fehler		

11. Vermutliche Motivation des Verursachers

□	strafbare Handlung / finanzieller Gewinn	□	Zeitvertreib / Hacking
□	politisch / terroristisch	□	Rache
□	Andere Welche:		

12.Durchgeführte Maßnahmen zur Behandlung des IT-Sicherheitsvorfalls

voraussichtlicher Beginn der Maßnahme	voraussichtliche Beendigung der Maßnahme	Beschreibung der geplanten Maßnahme

13.Geplante Maßnahmen zur Behandlung des IT-Sicherheitsvorfalls

voraussichtlicher Beginn der Maßnahme	voraussichtliche Beendigung der Maßnahme	Beschreibung der geplanten Maßnahme

14.Ausstehende Maßnahmen

15.Zusammenfassende Bewertung des IT-Sicherheitsvorfalls

□ Hohe Bedeutung

□ Geringe Bedeutung

Kurze Begründung bzw. andere Bewertung

16.Benachrichtigte Personen / Institutionen

Register der benachrichtigten Personen	□	Management	□	externe Dienstleister
	□	Sicherheitsbeauftragter/ Datenschutzbeauftragter	□	Strafverfolgungsbehörden
	□	EDÖB	□	Ärztekasse
	□	Mitglieder des Expertenteams	□	Andere Welche:

17.Unterschriften der involvierten Personen

Vor- und Nachname	Antonio Quirino
Funktion	Einzelunternehmer, Arzt
Datum	
Unterschrift	

Vor- und Nachname	
Funktion	
Datum	
Unterschrift	

Vor- und Nachname	
Funktion	
Datum	
Unterschrift	

Vor- und Nachname	
Funktion	
Datum	
Unterschrift	

Vor- und Nachname	
Funktion	
Datum	
Unterschrift	