Notfallmanagement Datenschutz

## Zweck

Diese SOP beschreibt das Notfallmanagement der Viva Hub AG nach den Empfehlungen des Bundesamts für Cybersicherheit der Schweiz (BACS). Ziel ist es, eine strukturierte und effiziente Reaktion auf Cyberangriffe oder Sicherheitsvorfälle zu gewährleisten, um Schäden zu minimieren und eine sichere Wiederherstellung der Systeme zu ermöglichen.

## Anwendungsbereich

Diese SOP gilt für alle Mitarbeitenden und IT-Systeme der Viva Hub AG und betrifft alle Massnahmen zur Datensicherheit und zum Schutz sensibler Daten vor Cyberangriffen.

## Verantwortlichkeiten

* Datenschutzbeauftragte.r: Überwacht und koordiniert alle Reaktionen auf Sicherheitsvorfälle.
* Mitarbeitende: Folgen den Sicherheitsvorgaben und Schulungen; melden verdächtige Aktivitäten an die zuständige Stelle.
* Geschäftsführung: Stellt die Bereitstellung der erforderlichen Ressourcen sicher und übernimmt die Entscheidungsverantwortung für Restrisiken.

## Definitionen

* BACS: Bundesamt für Cybersicherheit der Schweiz, das Cybersicherheitsstandards für KMUs bereitstellt.
* Malware: Schädliche Software wie Viren und Trojaner, die die Sicherheit des Netzwerks gefährden kann.

## Materialien und Ausrüstung

* Externe, isolierte Backup-Festplatte
* Antiviren- und Sicherheitssoftware
* Passwort-Manager

## Sicherheits- und Gesundheitshinweise

Die Mitarbeitenden sind angewiesen, keine unautorisierten USB-Sticks zu verwenden und keine verdächtigen E-Mails zu öffnen, um eine Malware-Infektion zu verhindern. Potenzielle Bedrohungen und schädliche Anhänge werden durch Spam-Filter und Sicherheitssoftware blockiert.

## Verfahrensbeschreibung

#### Vorbeugende Massnahmen

* **Regelmässige Datensicherungen**: Durchführung täglicher Backups auf einer externen, physisch getrennten Festplatte oder einem Cloud-Speicher. Die Backup-Festplatte ist nach jedem Backup physisch zu trennen.
* **Schulung der Mitarbeitenden**: Schulungen zu IT-Sicherheitsgrundlagen, basierend auf BACS-Empfehlungen. Mitarbeitende lernen, verdächtige Mails zu erkennen und Sicherheitsrisiken durch USB-Sticks zu vermeiden.
* **Passwortmanagement**: Verwendung eines Passwort-Managers und Einsatz von sicheren Passwörtern. Zweifaktor-Authentifizierung (2FA) ist für kritische Systeme erforderlich.
* **Erstellung eines Notfallplans**: Dokumentierte, regelmässig aktualisierte Anweisungen für den Umgang mit Sicherheitsvorfällen.

#### Erkennung und schnelle Reaktion

1. **Erkennen eines Sicherheitsvorfalls**: Überwachung des Netzwerks und frühzeitige Identifizierung verdächtiger Aktivitäten, wie unautorisierte Zugriffe oder Anomalien im Netzwerkverkehr.
2. **Alarm auslösen**: Im Falle eines Malware-Falls wird ein interner Alarm ausgelöst und die IT-Abteilung benachrichtigt.

#### Erste Notfallmassnahmen bei Malware-Infektion

1. **Netzwerk isolieren**: Alle betroffenen Geräte vom Netzwerk trennen; WLAN und Kabelverbindungen kappen.
2. **Keine zusätzlichen Geräte einschalten**: Keine weiteren Geräte verbinden, bis die Bedrohung entfernt ist.
3. **Keine Backup-Festplatten anschliessen**: Die Backup-Festplatten erst nach vollständiger Bereinigung des Netzwerks anschliessen.

#### Malware-Analyse und -Entfernung

1. **Malware identifizieren**: Mithilfe der Sicherheitssoftware oder durch externe Experten die Malware analysieren.
2. **Bereinigung und Desinfektion**: Betroffene Systeme vollständig bereinigen, ggf. Systemscan und Neuinstallation vornehmen.
3. **Überprüfung des gesamten Netzwerks**: Sicherstellen, dass keine anderen Geräte infiziert sind.

#### Wiederherstellung und Schutzmassnahmen

1. **Sichere Wiederherstellung**: Backup-Festplatte anschliessen und die Daten wiederherstellen, sobald das Netzwerk gesichert ist.
2. **Passwörter ändern**: Alle Passwörter unmittelbar nach dem Vorfall ändern.
3. **Erneute Netzwerkintegration**: Geräte nach Überprüfung schrittweise wieder ins Netzwerk integrieren.

#### Nachbereitung und Prävention

1. **Vorfall dokumentieren**: Alle Details des Vorfalls und der getroffenen Massnahmen dokumentieren.
2. **Systemupdates und Patches**: Software und Systeme auf dem neuesten Stand halten, Sicherheitslücken umgehend schliessen.
3. **Schulung und Sensibilisierung**: Mitarbeitende regelmässig zu neuen Bedrohungen und Präventionsmassnahmen schulen.

## Qualitätskontrolle

Regelmässige Überprüfung und Aktualisierung dieser SOP sowie Testläufe für die Notfallmassnahmen. Die Effektivität der SOP wird durch Tests und Schulungen bewertet.

## Dokumentation und Aufzeichnungen

CIRS, Backup-Logs und Schulungsnachweise werden zentral gespeichert und archiviert.

## Anhänge

Keine

## Revisionen und Änderungen

Keine