# CVD-Richtlinie des Main-Kinzig-Kreises

# (Coordinated Vulnerability Disclosure)

Als Kreisverwaltung hat für uns die Sicherheit von IT-Systemen und den zu verarbeitenden Informationen höchste Priorität. Schwachstellen und Sicherheitslücken können trotz sorgfältiger Arbeitsweise und technischer Schutzmaßnahmen nicht vollumfänglich ausgeschlossen werden. Daher ist es wichtig Schwachstellen frühzeitig zu erkennen und zu schließen. Wir unterstützen deswegen die verantwortungsvolle Meldung von Sicherheitslücken.

Sollten Sie eine oder mehrere Schwachstellen in IT-Systemen des Main-Kinzig-Kreises gefunden haben, können Sie sich vertrauensvoll an uns wenden. Wir nehmen jede gemeldete Schwachstelle ernst.

## Meldung von Schwachstellen

Gefundene Schwachstellen können per E-Mail an it-sicherheit@mkk.de gemeldet werden. Dabei ist es wünschenswert, wenn möglichst viele Informationen zu der Schwachstelle selbst mitgeteilt werden:

- Beschreibung der Schwachstelle
- betroffenes System
- Schritte zur Reproduktion
- potenzielle Auswirkungen
- technische Nachweise (falls vorhanden)

Die Übermittlung der Informationen kann gesichert über verschlüsselte E-Mails erfolgen. Entsprechende Informationen dazu sind auf folgender Seite erhältlich:

https://www.mkk.de/de/mkk_de/technische_inhalte/Datenschutz.html

## Eingehende Meldungen

Wenn eine Meldung über eine Schwachstelle bei uns eingegangen ist, gehen wir wie folgt vor:

- Wir behandeln jeden Schwachstellenbericht innerhalb des gesetzlichen Rahmens vertraulich.
- Wir geben die personenbezogenen Daten der meldenden Person nicht ohne Zustimmung an Dritte weiter.
- Wir bewerten die Schwachstelle und leiten entsprechende Maßnahmen ein.
- Wir geben der meldenden Person eine Rückmeldung bzw. gehen über die Kontaktdaten aus der eingehenden E-Mail in einen Austausch.

## Regeln für Meldende

Wir sind dankbar für das Melden einer Schwachstelle, allerdings erwarten wir, dass folgende Grundsätze eingehalten werden:

- Die gefundene Schwachstelle wird und wurde nicht missbräuchlich ausgenutzt.
- Es werden und wurden keine Schäden über die gemeldete Schwachstelle angerichtet.
- Es werden und wurden keine Angriffe, wie DDOs, Social-Engineering, Brute-Force, etc. durchgeführt.
- Es werden und wurden keine Manipulationen oder Kompromittierung von Systemen oder Daten vorgenommen.
- Es werden oder wurden keine Informationen über die Schwachstelle an Dritte weitergegeben, die Dritte zur Ausnutzung der Schwachstelle nutzen können.
- Die Information über die Schwachstelle wird vertraulich behandelt, zumindest bis diese behoben wurde.

## Rechtliche Hinweise

Wenn eine meldende Person in gutem Glauben handelt, sich an diese Richtlinie und die Grundsätze hält und keine Schäden verursacht, werden wir keine strafrechtlichen Schritte einleiten. Sollten allerdings kriminelle Absichten verfolgt worden sein oder verfolgt werden, werden wir strafrechtliche Schritte einleiten.

Diese Richtlinie stellt keine rechtliche Zusicherung oder Haftungsfreistellung dar.

## Transparenz zu Gegenleistungen (Bug-Bounty)

Als öffentliche Verwaltung unterliegen wir haushaltsrechtlichen Vorgaben. Aus diesem Grund können für das Melden von Schwachstellen keine Gegenleistungen, weder materiell noch finanziell, gewährt werden. Somit stellt die CVD-Richtlinie kein Bug-Bounty-Programm dar.

Wir danken dennoch allen Personen, die durch verantwortungsvolles Melden aufgedeckter Schwachstellen zur Sicherheit unserer IT-Systeme beitragen.