Operatives Dokument · vom Gemeindeschreiber zu erlassen

Notfallkonzept

VERSION	ERLASSEN	IN KRAFT AB	KLASSIFIZIERUNG
1.0	15.02.2027	01.03.2027	intern, Anhang A vertraulich

VERSION	DATUM	BESCHREIBUNG	NAME
0.1	25.01.2027	Entwurf erstellt	Elchi Studios
1.0	15.02.2027	Erlassen	Beat Beispiel

1 Allgemeine Bestimmungen

1.1 Zweck

Das Notfallkonzept legt fest, wie die Politische Gemeinde Musterwil bei schweren Störungen, Sicherheitsvorfällen und Notfällen handelt. Ziel ist, Menschen zu schützen, Schäden zu begrenzen, gesetzliche Meldepflichten einzuhalten und die wichtigsten Dienstleistungen für die Bevölkerung so schnell wie möglich wieder bereitzustellen.

1.2 Geltungsbereich

Das Konzept gilt für die gesamte Verwaltung und für alle Ereignisse, die Informationen, IKT-Systeme, Gebäude oder Personal der Verwaltung betreffen. Für Ereignisse, die die ganze Bevölkerung betreffen (zum Beispiel Naturkatastrophen), gilt zusätzlich die Planung des Gemeindeführungsstabs Musterwil.

1.3 Grundlagen

- IDG (LS 170.4), insbesondere § 7 (Informationssicherheit) und § 12a (Meldung von Datenschutzvorfällen an die Datenschutzbeauftragte)
- Bundesgesetz über die Informationssicherheit beim Bund (ISG, SR 128), Art. 74a ff. (Meldepflicht für Cyberangriffe, gilt auch für Gemeindeverwaltungen), und Cybersicherheitsverordnung
- Allgemeine Richtlinie, Kapitel 8.17 und 8.21; Technische Richtlinie, Kapitel 13 und 18
- Bedrohungsanalyse und Schutzbedarfsanalyse der Politischen Gemeinde Musterwil
- BSI-Standard 200-4 (Business Continuity Management) als Orientierung

2 Notfallorganisation

2.1 Rollen

Rolle	Person	Stellvertretung	Aufgaben	Kompetenzen
Leitung Notfallorganisation	Beat Beispiel, Gemeindeschreiber	Carla Vorlage	Lage beurteilen, Notfall ausrufen und beenden, Massnahmen anordnen, Gemeinderat informieren	Ressourcen und Ausgaben bis CHF 20'000 freigeben, externe Hilfe aufbieten, Meldungen an Datenschutzbeauftragte und BACS auslösen
IKT-Koordination	Daniel Platzhalter, ISV	Eva Entwurf	Vorfall technisch beurteilen, IKT-Dienstleister steuern, Beweise sichern lassen, Wiederherstellung koordinieren	Systeme vom Netz nehmen lassen, Zugänge sperren, Notfallzugang im Tresor öffnen (zusammen mit Leitung)
Datenschutz	Franziska Muster, Datenschutzberaterin	Hanna Halter	Prüfen, ob Personendaten betroffen sind, Meldung an die Datenschutzbeauftragte vorbereiten, Information betroffener Personen vorbereiten	Kontakt mit der Datenschutzbeauftragten
Kommunikation	Anna Muster, Gemeindepräsidentin	Georg Gerüst, Vizepräsident	Medien, Bevölkerung und Behörden informieren, Textvorlagen anpassen	einzige Stelle für Medienauskünfte
Protokoll und Assistenz	Hanna Halter, Kanzlei	Ivo Inhalt, Kanzlei	Ereignisprotokoll führen (Anhang B), Kontakte herstellen, Logistik	gemäss Auftrag der Leitung
Fachbereiche	Abteilungsleitungen	gemäss Stellvertretungsregelung	Notbetrieb ihrer Abteilung gemäss Kapitel 5 organisieren	Prioritäten in der Abteilung setzen
Externe Unterstützung	Muster Informatik AG; bei Cyberangriffen der Incident-Response-Partner der Cyberversicherung	gemäss Vertrag	Analyse, Eindämmung, Wiederherstellung	gemäss Auftrag der IKT-Koordination

Der Gemeinderat hat den Notfallkredit von CHF 20'000 vorab bewilligt (GRB 2027-046), damit im Ernstfall nicht auf eine Sitzung gewartet werden muss.

2.2 Alarmierung

1. Wer einen Vorfall bemerkt, meldet ihn sofort der ISV (Telefon 044 000 00 10), bei Nichterreichen der Stellvertretung, danach dem Gemeindeschreiber.
2. Ausserhalb der Bürozeiten gilt die Notfallnummer 044 000 00 99 (Pikett Muster Informatik AG).

3. Bei Gefahr für Leib und Leben zuerst die Blaulichtorganisationen alarmieren: Polizei 117, Feuerwehr 118, Sanität 144.
4. Die ISV beurteilt die Stufe (Kapitel 6.1) und informiert bei Stufe 3 oder 4 sofort die Leitung Notfallorganisation.
5. Die Leitung bietet die Notfallorganisation auf (Telefonkette gemäss Anhang A).

3 Notfallinfrastruktur

3.1 Lagezentrum und Ausweichstandorte

Ereignis	Lagezentrum / Ausweichstandort	Benötigte Hilfsmittel
Evakuation	Sammelplatz Dorfplatz vor dem Gemeindehaus	Mobiltelefone, Personalliste
Gemeindehaus nicht benutzbar	Schulhaus Dorf, Lehrerzimmer	Notfallordner, Notebooks, Mobiltelefone, Mobilfunk-Router
Stromausfall im Gemeindehaus	Feuerwehrlokal Musterwil (Notstrom)	Notfallordner, Notebooks mit geladenem Akku, Mobiltelefone
Ausfall der Informatik (Gemeindehaus benutzbar)	Sitzungszimmer 1. OG	Notfallordner, Papierformulare, ausgedruckte Kontaktlisten
Cyberangriff	Sitzungszimmer 1. OG; Kommunikation nur über Mobiltelefone, nicht über das möglicherweise kompromittierte E-Mail	Notfallordner, Mobiltelefone, nicht betroffene Geräte

3.2 Notfallordner

Der Notfallordner liegt ausgedruckt an zwei Orten: im Tresor der Kanzlei (im Gemeindehaus) und beim Gemeindeschreiber zu Hause (ausserhalb). Er enthält mindestens:

- dieses Notfallkonzept,
- die Kontaktliste (Anhang A) mit privaten Mobilnummern der Notfallorganisation,
- die Personalliste mit Notfallkontakten,
- die Liste der Fachanwendungen mit Anbieter, Supportnummer und Kundennummer,
- Vertragsnummern und Supportzugänge (ohne Passwörter) des IKT-Dienstleisters, der Versicherung und des Webhosters,
- die Vorlage für das Ereignisprotokoll (Anhang B),
- Papierformulare für den Notbetrieb (zum Beispiel Quittungen, Anmeldungen),
- die Kurzanleitung für die Rufumleitung der Telefonzentrale.

Passwörter für den Notfallzugang liegen nicht im Notfallordner, sondern versiegelt im Tresor (Technische Richtlinie, Kapitel 4.3). Die ISV aktualisiert den Notfallordner halbjährlich.

4 Szenarien

Die vollständige Bewertung der Bedrohungen steht in der Bedrohungsanalyse. Für die Notfallplanung sind diese Szenarien massgebend:

Szenario	Bedrohungen	Checkliste
Ransomware oder anderer Cyberangriff	B23, B29, B38	7.1

Szenario	Bedrohungen	Checkliste
Kompromittiertes E-Mail-Konto oder Phishing mit eingegebenen Zugangsdaten	B27, B28	7.2
Datenschutzvorfall (Fehlversand, Verlust, unberechtigter Zugriff)	B16, B17, B19, B21	7.3
Ausfall von Internet, Leunet, IKT-Dienstleister oder Fachanwendung	B12, B13, B32	7.4
Stromausfall	B08, B11	7.5
Gemeindehaus nicht benutzbar (Brand, Wasser, Sperrung)	B01, B04, B06, B07	7.6
Ausfall von Schlüsselpersonen	B09, B10	Stellvertretungsregelung

5 Wiederanlauf-Prioritäten

Festgelegt im Analyse-Workshop vom 2. Februar 2027 mit den Abteilungsleitungen. Die tolerierbaren Ausfallzeiten stimmen mit der Schutzbedarfsanalyse und der Technischen Richtlinie überein.

Prio	Dienstleistung / Prozess	Benötigte Anwendungen	Tolerierbare Ausfallzeit	Notbetrieb ohne IKT
1	Erreichbarkeit der Verwaltung (Telefon, Hinweis auf der Website)	Telefonie, Website	4 Stunden	Rufumleitung auf Mobiltelefone, Hinweis auf der Website über den Webhoster
1	Bestattungswesen (Todesfälle)	Einwohnerkontrolle, Bestattungsmodul	1 Arbeitstag	Papierformulare, telefonische Absprache mit Bestattungsamt und Zivilstandsamt
1	Sozialhilfe: Auszahlung von Unterstützungsleistungen	Sozialhilfe-Anwendung, E-Banking	2 Arbeitstage	manuelle Zahlung gemäss Liste, Kollektivunterschrift
2	Einwohnerdienste (An- und Abmeldungen, Bestätigungen)	Einwohnerkontrolle	3 Arbeitstage	Meldungen auf Papier aufnehmen, später erfassen
2	Zahlungsverkehr (Kreditoren, Löhne)	Finanz- und Lohnanwendung, E-Banking	5 Arbeitstage, vor dem Lohnlauf 1 Tag	Lohnzahlung des Vormonats wiederholen lassen (Absprache mit der Bank)
2	Gemeinderatsgeschäfte, Protokolle	Geschäftsverwaltung	5 Arbeitstage	Papier, Sitzung verschieben
3	Steuern	Steueranwendung	10 Arbeitstage	Fristen verlängern
3	Bauverwaltung	Bauverwaltungsanwendung	10 Arbeitstage	Fristen verlängern
Sonderfall	Wahlen und Abstimmungen	Einwohnerkontrolle (Stimmregister)	in Wahlwochen 4 Stunden	Absprache mit Bezirk bzw. Statistischem Amt, Ausdruck des Stimmregisters vor dem Wahltag

6 Notfallprozess

6.1 Stufen

Stufe	Bezeichnung	Beispiel	Führung
1	Störung	einzelner Arbeitsplatz oder Drucker fällt aus	Support des IKT-Dienstleisters
2	Sicherheitsvorfall	Phishing-Klick ohne Folgen, verlorener verschlüsselter USB-Stick, Fehlversand an eine Behörde	ISV
3	Notfall	Ransomware auf einem Gerät, kompromittiertes Postfach, Ausfall einer Kernanwendung länger als tolerierbar, Datenschutzvorfall mit Meldepflicht	Leitung Notfallorganisation
4	Krise	Verwaltung weitgehend arbeitsunfähig, Datenabfluss an die Öffentlichkeit, grosses Medieninteresse	Leitung Notfallorganisation und Gemeinderat

6.2 Ablauf

1. **Erkennen und melden:** Der Vorfall wird der ISV gemeldet (Kapitel 2.2). Ereignisprotokoll beginnen (Anhang B): Zeitpunkt, wer, was beobachtet.
2. **Beurteilen:** Die ISV bestimmt Stufe und betroffene Systeme, Daten und Personen. Bei Stufe 3 und 4 wird die Notfallorganisation aufgeboten.
3. **Sofortmassnahmen:** Schaden eindämmen (Szenario-Checkliste in Kapitel 7), Menschen schützen, Beweise sichern.
4. **Meldepflichten prüfen:** in den ersten Stunden prüfen und auslösen (Kapitel 6.3).
5. **Kommunizieren:** gemäss Kommunikationsmatrix (Kapitel 8), intern zuerst.
6. **Notbetrieb:** Die Abteilungen arbeiten nach Kapitel 5.
7. **Wiederherstellen:** Systeme nach Prioritäten wiederherstellen, erst nach Freigabe durch die IKT-Koordination wieder ans Netz.
8. **Beenden:** Die Leitung erklärt den Notfall für beendet und informiert alle Beteiligten.
9. **Nachbearbeiten:** innert 30 Tagen Bericht mit Ursache, Verlauf, Kosten und Verbesserungsmassnahmen; Massnahmen in den Massnahmenkatalog übernehmen; Bedrohungsanalyse und Notfallkonzept anpassen.

6.3 Meldepflichten

Stelle	Wann	Frist	Wer meldet	Wie
Datenschutzbeauftragte des Kantons Zürich	Personendaten wurden unbefugt bearbeitet, bekannt gegeben oder gingen verloren, und Grundrechte betroffener Personen sind gefährdet (§ 12a IDG); im Zweifel melden	unverzüglich	Gemeindeschreiber, vorbereitet durch Datenschutzberatung	Meldeformular auf datenschutz.ch oder datenschutz@dsb.zh.ch
Bundesamt für Cybersicherheit (BACS)	Cyberangriff, der die Funktionsfähigkeit gefährdet, zu Abfluss oder Manipulation von Informationen geführt hat, mit Erpressung, Drohung oder Nötigung verbunden ist oder lange unentdeckt blieb	innert 24 Stunden nach Entdeckung; Ergänzungen innert 14 Tagen	ISV	Meldeportal des BACS

Stelle	Wann	Frist	Wer meldet	Wie
Kantonspolizei Zürich	strafbare Handlung (Cyberangriff, Erpressung, Diebstahl, Betrug)	so rasch wie möglich	Gemeindeschreiber	Notruf 117 bei akuter Gefahr, sonst Anzeige
Versicherung	Schadenfall gemäss Police (Cyber, Sach, Haftpflicht)	gemäss Police, oft 24 bis 72 Stunden	Gemeindeschreiber	Schadenhotline der Muster Versicherung AG
Betroffene Personen	wenn es zu ihrem Schutz nötig ist oder die Datenschutzbeauftragte es verlangt	so rasch wie möglich	Gemeindeschreiber, vorbereitet durch Datenschutzberatung	Brief bzw. E-Mail gemäss Textvorlage
Leunet-Betreiber bzw. Kanton	Vorfall könnte das kantonale Netz betreffen	sofort	ISV	gemäss Anschlussvereinbarung
Bezirksrat Affoltern	Krise mit erheblichen Auswirkungen auf die Aufgabenerfüllung	innert Tagesfrist	Gemeindepräsidentin	Telefon und schriftlich

Seit dem 1. Oktober 2025 kann die Verletzung der Meldepflicht an das BACS mit Busse bestraft werden. Die ISV prüft die Kriterien bei jeder Überprüfung des Konzepts auf der Website des BACS nach.

7 Szenario-Checklisten

7.1 Ransomware oder anderer Cyberangriff

- Betroffene Geräte sofort vom Netz trennen (Kabel ziehen, WLAN aus), nicht ausschalten.
- ISV und IKT-Dienstleister alarmieren; bei Verdacht auf Ausbreitung Internetverbindung und VPN sperren lassen.
- Notfallorganisation aufbieten (Stufe 3 oder 4), Kommunikation nur über Mobiltelefone.
- Incident-Response-Partner und Versicherung beiziehen.
- Beweise sichern lassen (Protokolle, Erpresserschreiben, Zeitpunkte), bevor Systeme neu aufgesetzt werden.
- Alle Passwörter von Administratoren und betroffenen Benutzern zurücksetzen, Zwei-Faktor-Methoden neu registrieren.
- Meldungen: BACS innert 24 Stunden, Kantonspolizei, Datenschutzbeauftragte, falls Personendaten betroffen sind.
- Kein Lösegeld zahlen und keinen Kontakt mit den Tätern ohne Absprache mit Polizei und Incident-Response-Partner.
- Prüfen, ob Daten abgeflossen sind (Leak-Seiten durch den Partner überwachen lassen).
- Wiederherstellung aus der unveränderbaren Sicherung nach Prioritäten (Kapitel 5), erst nach Bereinigung.
- Mitarbeitende, Gemeinderat und Bevölkerung gemäss Kommunikationsmatrix informieren.

7.2 Kompromittiertes E-Mail-Konto

- Passwort sofort zurücksetzen, alle Sitzungen abmelden, Zwei-Faktor-Methoden prüfen und neu registrieren.
- Weiterleitungs- und Posteingangsregeln prüfen und entfernen (ein häufiges Merkmal von Angriffen).
- Prüfen, welche E-Mails im Namen der Person verschickt wurden; Empfängerinnen und Empfänger warnen.
- Prüfen, auf welche Postfächer, Ablagen und Anwendungen das Konto zugreifen konnte (Datenabfluss?).
- Bei offenen Zahlungen: Bank informieren, Zahlungen der letzten Tage prüfen.

- Meldepflichten prüfen (Datenschutzbeauftragte, BACS).

7.3 Datenschutzvorfall

- Klären: Was ist passiert, welche Daten, wie viele Personen, wer hat Kenntnis erhalten?
- Schaden begrenzen: Empfänger um Löschung und Bestätigung bitten, Freigabelinks entfernen, Gerät sperren bzw. löschen.
- Die Datenschutzberatung beurteilt die Gefährdung der Grundrechte; der Gemeindeschreiber entscheidet über die Meldung an die Datenschutzbeauftragte (unverzüglich, im Zweifel melden).
- Information der betroffenen Personen prüfen.
- Vorfall im Vorfallregister dokumentieren, auch wenn keine Meldung erfolgt.

7.4 Ausfall von Internet, Leunet, IKT-Dienstleister oder Fachanwendung

- Störung beim Anbieter melden, Ticketnummer und voraussichtliche Dauer erfragen.
- Bei einem Ausfall von mehr als 2 Stunden: Ersatz-Internetverbindung (Mobilfunk-Router) aktivieren.
- Telefonie: Rufumleitung auf Mobiltelefone schalten.
- Notbetrieb gemäss Kapitel 5; Hinweis auf der Website.
- Bei einem Ausfall des IKT-Dienstleisters von mehr als 2 Arbeitstagen: Die Leitung entscheidet über den Beizug eines Ersatzdienstleisters; Notfallzugang aus dem Tresor verwenden.

7.5 Stromausfall

- Prüfen, ob nur das Gebäude oder die Region betroffen ist (Elektrizitätswerk Musterwil, 044 000 00 50).
- Die USV verschafft Zeit für das kontrollierte Herunterfahren; der IKT-Dienstleister fährt die Systeme vor Ort kontrolliert herunter.
- Bei mehr als 4 Stunden: Ausweichstandort gemäss Kapitel 3.1.
- Nach Rückkehr des Stroms: Systeme in der Reihenfolge Netzwerk, Server, Arbeitsplätze starten und prüfen.

7.6 Gemeindehaus nicht benutzbar

- Evakuation, Sammelplatz, Personal vollzählig?
- Ausweichstandort einrichten, Notfallordner Nr. 2 holen.
- Notebooks und Mobiltelefone beschaffen bzw. vom IKT-Dienstleister bereitstellen lassen; Zugriff auf Anwendungen in externen Rechenzentren prüfen.
- Bevölkerung über Website, Aushang und lokale Medien über den neuen Standort und die Erreichbarkeit informieren.
- Papierakten sichern lassen (Feuerwehr, Restaurierungsfirma für nasse Akten).

8 Kommunikation

8.1 Grundsätze

- **Intern vor extern:** Mitarbeitende und Gemeinderat erfahren es nicht aus den Medien.
- **Eine Stimme:** Nur die für die Kommunikation verantwortliche Person gibt Auskunft.
- **Fakten statt Vermutungen:** Nur gesicherte Informationen; offen sagen, was man noch nicht weiss.
- **Nichts für Angreifer:** keine technischen Details und keine Aussagen zu Lösegeld.
- **Anderer Kanal:** Bei Cyberangriffen nicht über das betroffene E-Mail-System kommunizieren.

8.2 Kommunikationsmatrix

E = bei Ereignis, T = innert Tagesfrist bzw. tägliches Update, W = innert Wochenfrist, leer = nicht vorgesehen.

Ereignisart	Beispiel	Blau-licht	Mitarbei-tende	Gemein-derat	DSB	BACS	Polizei	Medien	Betroffene	IKT, Versiche-rung
Höhere Gewalt	Brand, Wasser, Ausfall Gemeindehaus	E	E	E			E	T	T (Bevölke-rung)	E
Technisches Versagen	Ausfall IKT oder Strom länger als tolerierbar		E	T				bei Bedarf	T (Website)	E
Menschliche Fehlhandlung	Fehlversand, verse-hentliche Datenlöschung			T	E, falls melde-pflichtig				T	E
Vorsätzliche Handlung	Ransomware, Datenabfluss		E	E	E	E (24 h)	E	T	T	E
Vorsätzliche Handlung	Kompromittiertes Postfach		T	T	E, falls melde-pflichtig	E, falls melde-pflichtig	T		T (Empfän-ger warnen)	E
Vorsätzliche Handlung	Angriff auf Mitarbei-tende am Schalter	E	T	E			E	W		Versiche-rung T

8.3 Textvorlagen

Mitarbeitende (sofort, mündlich oder per SMS): «Wir haben eine schwere Störung bzw. einen Sicherheitsvorfall in der Informatik. Bitte benutzen Sie bis auf Weiteres keine Computer und kein E-Mail. Trennen Sie Ihr Gerät nicht vom Strom. Weitere Informationen folgen um [Uhrzeit] über [Kanal]. Auskünfte an Dritte gibt nur Anna Muster.»

Bevölkerung (Website, Aushang): «Die Gemeindeverwaltung Musterwil ist aufgrund einer technischen Störung zurzeit nur eingeschränkt erreichbar. Dringende Anliegen: Telefon 044 000 00 01. Todesfälle melden Sie bitte wie gewohnt telefonisch. Wir informieren laufend an dieser Stelle.»

Medien (erste Stellungnahme): «Die Gemeinde Musterwil hat am [Datum] einen Vorfall in ihrer Informatik festgestellt. Sie hat sofort Massnahmen ergriffen, Fachleute beigezogen und die zuständigen Stellen informiert. Ob Personendaten betroffen sind, wird abgeklärt. Die Verwaltung bleibt für dringende Anliegen erreichbar. Weitere Informationen folgen, sobald gesicherte Erkenntnisse vorliegen.»

Betroffene Personen (Brief): «Bei der Gemeinde Musterwil ist am [Datum] ein Vorfall eingetreten, bei dem folgende Daten von Ihnen betroffen sein könnten: [Datenarten]. Wir haben [Massnahmen]. Wir empfehlen Ihnen [Empfehlung]. Für Fragen erreichen Sie uns unter [Kontakt].»

9 Notfallübungen und Tests

Übung / Test	Häufigkeit	Verantwortlich
Tischtest (Szenario 7.1 oder 7.3 durchspielen)	jährlich	ISV
Wiederherstellung einer Kernanwendung aus der Sicherung	jährlich	IKT-Dienstleister, Protokoll an ISV
Rufumleitung auf Mobiltelefone	jährlich	ISV
Erreichbarkeit der Telefonkette (Anhang A)	halbjährlich	Protokoll und Assistenz

Übung / Test	Häufigkeit	Verantwortlich
Notfallzugang im Tresor (Umschlag unversehrt, Passwörter gültig)	jährlich	Gemeindeschreiber und ISV
Evakuation	gemäss Gebäudesicherheit	Liegenschaften

Datum	Übung / Test	Resultat	Massnahmen
12.06.2027	Tischtest Ransomware	Ablauf klar; private Mobilnummer der Stellvertretung ISV fehlte	Anhang A nachgeführt

10 Überprüfung

Die ISV überprüft das Notfallkonzept jährlich, nach jeder Übung und nach jedem Notfall. Geprüft werden Prozesse und Prioritäten, Ressourcen, Bedrohungen, Massnahmen, Personen und Kontaktdaten. Kontaktdaten werden bei jeder Personaländerung sofort nachgeführt.

11 Genehmigung und Inkrafttreten

Dieses Notfallkonzept wurde vom Gemeindeschreiber am 15. Februar 2027 erlassen und tritt am 1. März 2027 in Kraft.

GEMEINDESCHREIBER

Beat Beispiel

INFORMATIONSSICHERHEITSVERANTWORTLICHE PERSON

Daniel Platzhalter

Anhang A: Kontaktliste

Klassifizierung «vertraulich» (private Nummern). Ausgedruckt im Notfallordner, nicht auf der Website. Im Muster sind die privaten Nummern weggelassen.

Funktion	Name	Mobil	Telefon Geschäft
Leitung Notfallorganisation	Beat Beispiel		044 000 00 02
Stellvertretung Leitung	Carla Vorlage		044 000 00 03
IKT-Koordination (ISV)	Daniel Platzhalter		044 000 00 10
Stellvertretung ISV	Eva Entwurf		044 000 00 11
Datenschutzberatung	Franziska Muster		044 000 00 20
Kommunikation	Anna Muster		044 000 00 04
Protokoll und Assistenz	Hanna Halter		044 000 00 05

Externe Stelle	Zweck	Telefon	Kunden- / Vertragsnr.
Muster Informatik AG	Support und Notfall IKT	044 000 00 99	MI-4471
Incident-Response-Partner der Cyberversicherung	Vorfallbehandlung Cyberangriff	gemäss Police	CY-2027-118
Muster Gemeindesoftware AG	Fachanwendungen	044 000 00 60	MG-0932
Muster Web GmbH	Website, Hinweis aufschalten	044 000 00 70	MW-210
Muster Telecom AG	Telefonie, Rufumleitung	0800 000 000	MT-55120
Musterbank	Zahlungsverkehr, Sperrung E-Banking	044 000 00 80	Vertrag 1187
Muster Versicherung AG	Cyber- und Sachversicherung	0800 000 001	Police 77-3301
Datenschutzbeauftragte des Kantons Zürich	Meldung Datenschutzvorfall	datenschutz@dsb.zh.ch	
Bundesamt für Cybersicherheit (BACS)	Meldepflicht Cyberangriffe	Meldeportal	
Kantonspolizei Zürich	Notruf, Anzeige	117	
Elektrizitätswerk Musterwil	Stromausfall	044 000 00 50	
Elchi Studios	Grundschutz-Betreuung (Bürozeiten)	058 513 63 11	GS-2027-014

Anhang B: Ereignisprotokoll

Datum, Zeit	Ereignis / Feststellung	Entscheid / Massnahme	Wer	Erledigt

Datum, Zeit	Ereignis / Feststellung	Entscheid / Massnahme	Wer	Erledigt

Begriffe

Begriff	Bedeutung
Notfall	Ereignis, bei dem wichtige Dienstleistungen länger als tolerierbar ausfallen oder schwerer Schaden droht und die normale Organisation nicht ausreicht
Krise	Notfall, der die ganze Verwaltung betrifft oder grosse öffentliche Wirkung hat
Notbetrieb	eingeschränkte Weiterführung einer Dienstleistung mit Ersatzmitteln
RTO	Recovery Time Objective: maximal tolerierbare Ausfallzeit
RPO	Recovery Point Objective: maximal tolerierbarer Datenverlust
Ransomware	Schadsoftware, die Daten verschlüsselt und Lösegeld fordert, oft mit Datenabfluss