# Berlin Global Village

# Sicherheitskonzept

# Inhalt

# 1 Einleitung

Nicht nervig, nötig! Dieses Sicherheitskonzept dient der Prävention und dem Umgang mit sicherheitsrelevanten Herausforderungen im Berlin Global Village (BGV). **Ziel ist es, ein offenes, inklusives und sicheres Umfeld für alle Nutzer*innen zu gewährleisten, ohne übermäßige Kontrollmaßnahmen einzuführen.** Diskriminierung, unnötige Befragung, Überwachung oder Stereotypisierung aufgrund des Aussehens werden nicht akzeptiert.

Das Sicherheitskonzept balanciert Offenheit und Sicherheit. Durch gezielte Maßnahmen wird das Sicherheitsniveau erhöht, ohne eine restriktive Atmosphäre zu schaffen. Die Kombination aus technischer Infrastruktur, Sensibilisierung und proaktiver Prävention stellt eine nachhaltige Sicherheitsstrategie sicher. **Dieses Konzept und die hier dargelegten Standards sind für alle in Berlin Global Village tätigen Personen erforderlich.**

# 2 Risikofaktoren

Die folgenden Faktoren können die Sicherheit gefährden oder einen Schaden schlimmer machen. Sie machen das BGV und die Menschen im Zentrum anfälliger für Gefahren.

## 2.1 Physische

- Externe Bereiche: Hinterhof, Mülleimer, Elektrokästen, Dekoloniales Denkzeichnen
- Interne Bereiche: Eingänge, Erdgeschoss, WCs, Altbau, Notausgänge, Treppenhäuser
- Zusätzlich: Briefe und Pakete

## 2.2 Organisatorisch

- Fehlende Awareness und Nachlässigkeit im Zentrum
- Event- und unangekündigte Besucher*innen

## 2.3 Digitale

- Malware und Phishing
- Offenlegung privater Informationen / Schutz der Privatsphäre
- Datenschutzverletzung, Identitätsdiebstahl
- Mobbing und Cyberstalking

# 3 Bedrohungsakteure

Einzelpersonen oder Organisationen, die unter folgenden Bedrohungen stehen:

- **Diebstahl**: Kriminelle oder organisierte Banden, die sich unbefugt Zugang verschaffen, um Wertgegenstände oder vertrauliche Informationen zu stehlen.
- **Vandalismus**: Einzelpersonen oder Gruppen, die vorsätzlich Sachbeschädigungen verursachen, sei es aus Frustration, Protest oder Zerstörungswut.
- **Politisch motivierte Gewalt**: Extremistische Gruppen oder Einzelpersonen, die durch Angriffe, Sabotage oder Einschüchterung politische Ziele verfolgen.

Diese Bedrohungen erfordern gezielte Sicherheitsmaßnahmen, um Schäden zu minimieren und Gefahren frühzeitig zu erkennen.

# 4 Prozesse vor Ort

Berlin Global Village ist in erster Linie ein physischer Ort. Deshalb ist die Sicherheit aller Menschen hier, ihres Eigentums und des Zentrums selbst besonders wichtig. In diesem Abschnitt geht es darum, wie wir gemeinsam Verantwortung übernehmen und aufeinander achten können.

Da jederzeit etwas passieren kann und ein klarer Ablauf superwichtig ist, um schnell auf Sicherheitsprobleme zu reagieren, haltet euch im Notfall bitte an folgende Schritte:

1. **Sofort 112 oder 110 anrufen.** Die Hilfe ist meistens in 5–10 Minuten da.
   - 112: Für Rettungsdienst oder Feuerwehr – z. B. bei einem Brand oder Unfall.
   - 110: Für die Polizei – z. B. bei einem Verbrechen.
2. **Meldet euch bei der Geschäftsstelle -** 030 49 96 64 00
3. **Am Wochenende oder außerhalb der Bürozeiten:** Ruft die Notfallnummer des Zentrums an - 030 549 09 942 21

**Erste-Hilfe-Kästen** findest du auf jeder Etage in den Teeküchen und in das Eventbüro. Die BGV-Hausverwaltung kümmert sich darum, abgelaufene Inhalte zu ersetzen. Wenn etwas vorher aufgebraucht wird, ist die jeweilige Etage selbst dafür verantwortlich, das nachzufüllen.

**Ein Defibrillator** steht im Altbau im Erdgeschoss neben dem Aufzug für Notfälle bereit. Ein Anleitungsvideo zur Nutzung findest du auf der internen Website. Wir empfehlen allen Angehörigen des Zentrums, sich damit vertraut zu machen.

## 4.1 Kontrollierter Zugang zum Zentrum

Es gibt nur wenige Eingänge ins Gebäude – alle gehen über den Haupt- oder Hintereingang durch das Foyer. Alle anderen Türen haben Alarme und sind nur für Notfälle gedacht.

Das Transpondersystem mit Chipkarten sorgt dafür, dass nur autorisierte Personen Zutritt haben. **Gäste müssen im Foyer abgeholt und begleitet werden.**

Beachtet bitte, dass sich die automatische Tür am Haupteingang langsam schließt – das ist wichtig für Menschen mit eingeschränkter Mobilität. **Lasst niemanden ins Foyer, der nicht von der besuchten Organisation hereingelassen wurde.**

Außer bei laufendem Veranstaltungsbetrieb lassen sich die Türen vom Foyer zum Neubau oder ins Begegnungs-Café nur mit einem Transponder öffnen. Wer keinen funktionierenden Transponder hat, sollte nicht ohne Begleitung ins Gebäude gelangen – das gilt auch für den Fahrstuhl.

Bitte helft mit, indem ihr darauf achtet, dass:

- Nur autorisierte Personen mit euch in Räume oder den Fahrstuhl kommen.
- Beim Verlassen eines Raumes alle Fenster und Türen geschlossen (und wenn nötig abgeschlossen) sind.
- Beim Verlassen des Zentrums alle Türen (inklusive bei der Ludotek) geschlossen sind.

## 4.2 Einbruchschutz

Einbrüche – egal ob Diebstahl oder Vandalismus – sind teuer und stressig. Neben finanziellen Verlusten kann es auch das Sicherheitsgefühl im Zentrum beeinträchtigen. Deshalb tun wir alles, um Einbrüche zu verhindern.

Einige Räume im Erdgeschoss haben Alarmanlagen, die außerhalb der regulären Öffnungszeiten aktiv sind. Wenn ein Alarm ausgelöst wird, wird automatisch die Polizei informiert. Falls ihr versehentlich einen Alarm auslöst, meldet das sofort der Hausverwaltung.

Zusätzlich gibt es verstärkte Fenster, Flutlichter und einen höheren Zaun im hinteren Bereich, um Einbrüche zu erschweren.

## 4.3 Drogenkonsum im Zentrum

Drogenkonsum ist in unserer Nachbarschaft weit verbreitet, und es kann sein, dass Personen, die stark unter dem Einfluss einer Substanz stehen, im oder um das Zentrum herum anzutreffen sind. Wenn du merkst, dass jemand im Zentrum Drogen konsumiert oder stark beeinträchtigt ist, bleib ruhig und vermeide eine direkte Konfrontation. Sprich die Person nicht darauf an, wenn du dich dabei unsicher fühlst. Informiere sofort die Geschäftsstelle.

Du kannst dafür den nächsten Infopunkt (Eventbüro oder Verwaltungsbüro) aufsuchen oder die interne Nummer anrufen. Außerhalb unserer Geschäftszeiten, ist Rebax, der Nothausverwaltung unter 030 549 09 942 21 zu erreichen.

In den Anhängen findest du eine detaillierte Anleitung, was zu tun ist. Das kann allgemein eine nützliche Orientierung sein.

## 4.4 Sichere Annahme von Briefen und Paketen

Um Risiken durch gefälschte oder gefährliche Sendungen zu vermeiden, gibt es eine zentrale Paketannahmestelle. Das Eventbüro übernimmt diese Aufgabe und sorgt dafür, dass nur autorisierte Personen Pakete entgegennehmen. Eingehende Pakete können im Eventbüro täglich zwischen 14:00 und 16:00 Uhr abgeholt werden.

# 5 Besonders gefährdete Personengruppen

Frauen*, gender-nonkonforme Personen und Kinder sind potenziellen Bedrohungen wie Gewalt oder Diebstahl besonders ausgesetzt. Daher erfordert das Sicherheitskonzept besondere Schutzmaßnahmen, um Sicherheit und ein sicheres Umfeld zu gewährleisten.

Diskriminierung ist in unseren Richtlinien für Vielfalt und soziale Inklusion berücksichtigt.

## 5.3 Spezielle Maßnahmen für Frauen und gender-nonkonforme Personen

Frauen* und gender-nonkonforme Personen haben oft besondere Sicherheitsbedenken und sind teils besonderen Gefährdungen ausgesetzt – insbesondere in Bezug auf Belästigung und Übergriffe, vor allem an Wochenenden und in den Abendstunden.

- **Sichere Rückzugsräume:** Das BGV-Eventbüro im Foyer, der Ruheraum im 4. Stock des Neubaus und das Büro der Geschäftsführung stehen als geschützte Räume zur Verfügung. Das Eventbüro und das Büro der Geschäftsführung können genutzt werden, wenn Mitarbeitende der Geschäftsstelle vor Ort sind. Der Ruheraum ist jederzeit zugänglich.
- **Bewegungsgesteuerte Beleuchtung:** Zusätzliche Lichter in dunklen Bereichen wie dem Hinterhof, den Fahrradständern und den Eingängen erhöhen die Sicherheit.
- **Begleitnetzwerk:** Über WhatsApp kannst du im gesamten Gelände eine Begleitung organisieren, falls du dich unsicher fühlst. Einfach hier klicken, um die Gruppe beizutreten.
- **Notfallkontakte:** Sind dauerhaft im Foyer gegenüber dem Aufzug ausgehängt.

## 5.4 Spezielle Maßnahmen für Kinder

Kinder brauchen besonderen Schutz, da sie Gefahren oft nicht selbst erkennen oder richtig einschätzen können. Sie verlassen sich stark auf die Anleitung und den Schutz von Erwachsenen, insbesondere in unbekannten oder unübersichtlichen Umgebungen.

- **Kinderfreundliche Bereiche:** Bereiche wie Ludothek und EPIZ sind sicherer Zonen, in denen Kinder während ihres Besuchs im Zentrum leicht beaufsichtigt werden können. Diese Zonen sind für Eltern oder Erziehungsberechtigte gut erreichbar mit eigenen Öffnungszeiten.
- **Erwachsene Aufsicht erforderlich**: Kinder müssen von einem Erwachsenen begleitet werden. Gäste oder Organisationen, die Veranstaltungen ausrichten, sollten das Personal dazu anregen, besonders auf die Sicherheit von Kindern zu achten, vor allem bei Veranstaltungen, die Familien oder gemischte Altersgruppen anziehen.
- **Kinderschutz-Policy**: Organisationen, die Veranstaltungen für Kinder oder Jugendliche ohne elterliche Begleitung anbieten, benötigen eine Kinderschutz-Policy. Der Anti-Diskriminierungskodex des Berlin Global Village gilt ebenso für Kinder im Zentrum. Diskriminierung oder Gewalt jeglicher Art gegenüber Kindern soll umgehend der internen Anlaufstelle gemeldet werden.
- **Recht am eigenen Bild und Fotografieren von Kindern:** Es ist untersagt, Fotos oder Videos von Kindern zu machen oder zu veröffentlichen, ohne die ausdrückliche Einwilligung der Eltern oder Erziehungsberechtigten. Eine schriftliche Einwilligung muss vor der Veröffentlichung eingeholt werden, z. B. bei der Anmeldung zu Veranstaltungen.
- **Kennzeichnung von sicheren Ansprechpersonen**: Bei großen Veranstaltungen brauchen verantwortliche Personen, an die sich Kinder wenden können, eine sichtbare Identifikation (z.B. Awareness Team Westen)
- **Begrenzter Zugang zu sensiblen Bereichen**: Türen zu gefährlichen oder nicht kindgerechten Bereichen sind abgeschlossen und nur mit Transponder zugänglich.
- **Kindgerechte Erste-Hilfe-Kits**: Erste-Hilfe-Kits beinhalten Materialien, die für Kinder geeignet sind (z. B. Kinderpflaster, Anweisungen zur Behandlung kleinerer Verletzungen).

# 6 Organisatorische Prozesse

1 Notfallnummern hängen im ganzen Gebäude – an jedem Infopunkt und Aufzug. Du findest sie auch im internen Bereich auf der Website.

2 Evakuierungsrouten sind auf jedem Stockwerk und an jedem Notausgang angezeigt. Die Notausgangsrouten und Feuerlöschern sind gut gekennzeichnet.

3 Im Zentrum finden jedes Jahr in Frühling ein Info- und Trainingstreffen statt, um offen über Sicherheitsrisiken zu sprechen und das Zentrum für das Thema sichere Räume und den Umgang mit Belästigung zu sensibilisieren. Dieses Treffen umfasst Training für spezifische Sicherheitssituationen und schließt mit einer Evakuierungsübung ab.

4 Das Hausrecht bei Veranstaltungen wird in den Verhaltensstandards geklärt, die speziell für die Veranstaltungsproduktion und kurzfristige Gäste gelten.

## 6.1 Evakuierungen

Berlin Global Village verfügt über kein zentrales Alarmsystem, sondern nur eines im Erdgeschoss, das im gesamten Gebäude zu hören ist. Wenn das Alarmgerät im Erdgeschoss ausgelöst wird, ist dies das Signal, das Gebäude zu evakuieren. Es gibt einige Situationen, in denen eine Evakuierung eingeleitet werden sollte.

**Wann sollte evakuiert werden:**

- Brand, sichtbarer Rauch, Gasgeruch oder -austritt
- Strukturelle Schäden (z. B. Deckeneinsturz)
- Bombendrohung oder andere Sicherheitsbedrohungen
- Anweisung durch Einsatzkräfte

### 6.1.1 Evakuierungsverfahren

1. **Sofort 112 oder 110 anrufen und die Geschäftsstelle informieren.**
2. **Andere alarmieren:** Wenn du einen Vorfall feststellst, der eine sofortige Reaktion erfordert, kommuniziere laut, deutlich, einfach und ruhig, z. B.: „Feuer, bitte evakuieren."
3. **Evakuierungsrouten**: Auf jedem Stockwerk gibt es klar markierte Fluchtwege. Bitte benutze die Treppen und Notausgänge. Nutze im Notfall nicht den Aufzug. Bitte stellen sicher, dass alle Mitarbeiter*innen deine Organisation erfasst und informiert sind. Wenn möglich, auch die Etage.
4. **Vulnerable Gruppen**: Unterstütze Menschen mit Behinderungen, Kinder oder andere, die während der Evakuierung Hilfe benötigen, wenn möglich.
5. **Event-Besucher*innen**: Jeder Seminarraum beinhaltet eine Information für Gäste, um sicherzustellen, dass auch Besucher*innen sicher evakuiert werden, da sie sich möglicherweise nicht mit dem Layout des Zentrums auskennen.
6. **Treffen an Sammelstelle:** Gehe nach der Evakuierung, wenn möglich, zum Babette Biergarten (Haupt-Sammelstelle). Wenn das nicht möglich ist, versammle dich auf dem REWE-Parkplatz (Ausweich-Sammelstelle). Achte beim Verlassen des Gebäudes auf ankommende Einsatzfahrzeuge.

7. **Teamzählung an der Sammelstelle:** Sobald du an der Sammelstelle bist, sollte jede Gruppe (z. B. Organisation oder Event-Veranstalter) eine eigene Personenzählung durchführen. Die zugewiesenen Evakuierungsleitenden stellen sicher, dass jede Person mit ihrem Namen bei ihnen eincheckt.
8. **Notfalldienste:** Wenn nach allen Überprüfungen noch jemand vermisst wird, benachrichtige sofort die Notfalldienste. Gib ihnen den Namen, den letzten bekannten Standort und andere Details, um bei der Suche zu helfen.
9. **Wiedereintrittsprotokoll:** Erst nachdem der Rollcall abgeschlossen ist und das Gebäude von den Notfalldiensten freigegeben wurde, darf das Gebäude wieder betreten werden.

## 6.2 Evakuierungsübungen

Übung wird einmal im Jahr durchgeführt, damit alle wissen, was im Notfall zu tun ist. Nach jeder Übung wird Feedback gesammelt, um das Evakuierungsprotokoll zu verbessern und mögliche Probleme anzugehen.

## 6.3 Regelmäßige Überprüfung der elektrischen Betriebsmittel

Gemäß der DGUV Vorschrift 3 müssen alle Kabel zu den elektrischen Betriebsmitteln wie Notebooks, Monitore, Drucker, Wasserkocher und ähnliche Geräte regelmäßig auf ihre Sicherheit geprüft werden. Diese Prüfungen sind in der Regel alle 24 Monate durchzuführen und dienen dem Schutz aller Personen im Gebäude sowie der Einhaltung gesetzlicher Vorgaben.

Es ist wichtig zu wissen, dass bei Nichtbefolgung dieser Vorschrift erhebliche Haftungsrisiken, mögliche Sanktionen und Probleme beim Versicherungsschutz entstehen können. Um diese Risiken zu vermeiden und sicherzustellen, dass wir alle sicher und gesetzeskonform arbeiten, lässt die Geschäftsstelle alle 2 Jahre für das gesamte Gebäude und alle Mietenden eine zentrale Prüfung durchführen. Die dabei entstehenden Kosten werden im Rahmen der Betriebskosten auf alle Mieter umgelegt.

Bitte beachtet, dass diese Prüfungen unabhängig von der durch uns organisierten Sammelprüfung in eure Verantwortung fallen. Dies gilt insbesondere für den Zutritt zu allen Geräten beim Sammeltermin, bei Neuanschaffungen und bei Änderungen an elektrischen Geräten.

Bei der Prüfung läuft der Prüfer durch die Gebäude und Büros. Es muss nichts gesammelt werden, sondern nur zugänglich gemacht, damit alles getestet werden kann.

# 7 Cybersecurity Prozesse

## 7.1 Umfang und Ziel

Dokumentieren von Richtlinien zu dem Datenschutz und Vorbereitung auf und zum Umgang mit Cybersecurity Vorfälle. Dies umfasst Zuständigkeiten, Vorbereitungs- und Schulungsmöglichkeiten, Richtlinien für das direkte Handeln, zur Kommunikation, sowie zur Dokumentation im Nachhinein.

Die folgenden Cybersecurity-Maßnahmen gelten für die BGV-Geschäftsstelle, werden aber allen Organisationen im Zentrum empfohlen, sofern sie keine eigenen Cybersecurity-Richtlinien haben. Regelmäßige **Sicherheitsupdates**, **strenge Passwortvorgaben** und **Notfallpläne für Cyberangriffe** sind essenziell.

## 7.2 Zuständigkeiten

Diese Positionen müssen eine Vertretung haben, oder es muss auf andere Weise sichergestellt werden, dass sofort auf einen Vorfall reagiert werden kann.

**Kommunikationsbeauftragte:** Kommuniziert mit Mitarbeiter*innen und/oder Mieter*innen.

- Michaela: zischek@berlin-global-village.de, 0173 52 70 799
- Vertretung: Geschäftsführung (Molly)

**Vorfall Manager:** Koordiniert das Vorgehen im Fall eines Vorfalls und trifft Entscheidungen, sowie externen (Polizei, IT-Dienstleister/Oliver) Personen.

- Richard: ebertseder@berlin-global-village.de, 0176 45 88 42 97
- Vertretung: Geschäftsführung (Armin)

**IT-Verantwortliche:** Analysiert die IT-Infrastruktur, findet Schwachstellen und implementiert Lösungen.

- Oliver: or@berlin-global-village.de
- Vertretung: Lorena

## 7.3 Prävention

**Passwort Standards und Aufbewahrung**

- Passwörter dürfen nicht auf Zetteln/Papier auf beschrieben werden.
- Passwörter müssen innerhalb von 1Password hinterlegt werden (nur Passwort Manager und **keine** Browser Passwort Sicherung).
- Zufallsgenerierte Passwortfunktion von 1Password nutzen.
- Vermeide das Verwenden von persönlichen Informationen, Zahlen oder Buchstabenfolgen (123, abc, JKLÖ etc.) und auf jeden Fall das Wort „Passwort" in jeglicher Form.

**Browser standards**

- Standard browser: Firefox oder Microsoft Edge
- Two-Factor Authentification / 2FA: Einrichtung bei allen Personen, Programmen, Geräten wo es gibt.

## 7.4 Vorfällen

### 7.4.1 Angriffsmethoden

**Phishing**

Das erlangen von Passwörtern oder anderen kritischen und oder persönlichen Daten mithilfe eines „Köders". Diese Köder sind oft Emails, welche auf falsche Login Portale weiterleiten und dann die eingegebenen Daten stehlen.

https://www.youtube.com/watch?v=XgF42Jb8jxo Deutsch
https://www.youtube.com/watch?v=XsOWczwRVuc Englisch

**Malware**

Schadsoftware, die das Ziel hat, Daten von dem infizierten Computer zu erlangen. Alternativ wird der betroffene Computer verschlüsselt, und nur gegen Lösegeld freigegeben.

https://www.youtube.com/watch?v=KcDFN8s0QN8 Deutsch

Vorsicht: E-Mails sind eine beliebte Phishing Methode. Klicke auf keinen Fall auf einen Link in der Mail, sondern:

- Gehe sicher, dass diese E-Mails echt sind, indem du dir den Absender ansiehst.
- Gehe mit der Maus (ohne zu klicken) über die E-Mail-Adresse oder einen Link. Beim Hovern wird das wahre Ziel angezeigt.
- Gehe eigenständig auf die betroffene Website und ändere dein Passwort

### 7.4.2 Motiv

- Mobbing/Cyberstalking
- Identitätsdiebstahl
- Datenschutzverletzungen
- Offenlegung von privaten Informationen

## 7.5 Vorfalls Reaktion Prozess

1 **digital Footprint und Datenschutzprävention:**
   - Cookies Anfragen ablehnen
   - separaten Kontos für Dienste verwenden, oder wenn möglich Login vermeiden
   - Alternativen zu Google verwenden (Firefox, Ecosia/DuckDuckGo)
   - keine persönlichen Daten in Benutzernamen integrieren

Je größer und öffentlicher der digitale Footprint, desto leichter ist es Opfer von gezieltem Phishing oder Doxxing zu werden.

2 **Identifikation:** Wissen wie ein Vorfall aussieht und dieses Weiterleiten an alle drei Beauftragten. Wenn möglich/nötig, erste Isolationsversuche.

### 7.5.1 Anzeichen für einen Vorfall:

- ungewöhnlich langsamer Laptop: Dies kann darauf hinweisen, dass im Hintergrund Schadsoftware läuft und Ressourcen verwendet.
- unerwartete Pop-Ups, vor allem wenn diese nicht auf einer Website erscheinen und dich zu Sachen auffordern z.B. Einen Support zu kontaktieren.
- Neue unbekannte Anwendungen: Normalerweise haben nur Admins Rechte, um Software zu installieren. Software die du nicht installiert hast, kann Schadsoftware sein. Deinstalliere diese oder, frage nach was es ist, wenn du dir nicht sicher bist.
- Verdächtige Prozesse: Prozesse die im Task-Manager laufen die dir verdächtig erscheinen, können auf installierte Schadsoftware hinweisen.
- Ungewohntes verhalten von Anwendungen: Wenn Programme häufiger abstürzen oder dich auf Websites weiterleiten (z.B. im Falle des Browsers).
- Warnmeldungen: achte auf Benachrichtigungen der Antivirensoftware (Bei BGV: Windows Viren- und Bedrohungsschutz), und darauf ob Sicherheitsoptionen in den Einstellungen plötzlich deaktiviert sind.
- Ungewöhnliche Kontaktdaten Aktivitäten: Emails mit Benachrichtigungen zu neu angemeldeten Geräten oder Passwortänderungen.

### 7.5.2 Eindämmung

Isolation des Vorfalls, um das Weiterverbreiten auf andere Infrastruktur zu vermeiden.

**Erste Schritte**

- Internetverbindung trennen: WLAN deaktivieren
- Zuständige Personen informieren
- Virenscan durchführen
- Passwörter ändern
- System aktualisieren

**Malware**

- Verdächtige IP-Adressen und Ports sperren
- Höhere Sicherheitsstufe in Sicherheitssoftware, Antivirensoftware und Firewall aktivieren, um Analyse betreiben zu können

**Phishing**

- Betroffene Zugangsdaten ändern
- Alle eingeloggten Geräte aus Accounts ausloggen

### 7.5.3 Behebung

Beseitigung des Vorfalls und dessen Ursache, sowie Wiederherstellen der Systeme. Diese Aktionen werden je nach Vorfall sehr unterschiedlich sein. Die Behebung von Vorfällen ist Sache des IT-Verantwortlichen (Oliver) und nicht des Endnutzers.

## 7.6 Wiederherstellung

Rückkehr zum Normalbetrieb und weitere Überwachung der Systeme. **Das macht nur der IT.**

- Verwendung von sicheren Backups, um zu verhindern das die Schwachstelle wieder ins System gerät.
- Aktualisieren der Zugangsdaten der betroffenen Systeme, falls nicht bereits geschehen, dabei darauf achten, dass das neue Passwort sowohl stark und vor allem **anders** als das alte ist.
- Sicherheitstests: Betroffene Systeme sollten vor der Wiederinbetriebnahme einem Sicherheitstest unterzogen werden, um sicherzustellen das die vorhandenen Sicherheitslücke geschlossen wurde und keine weiteren bestehen.
- Mitarbeiter sollten nach Wiederherstellung testen, ob alles so funktioniert wie vor dem Vorfall.
- Eine gezieltere Überwachung der betroffenen Systeme und der genutzten Schwachstellen.

## 7.7 Nachbereitung:

Analyse des Vorfalls und des Vorgehens, Dokumentation der Geschehnisse und Verbesserung des IRPs (Vorfall Reaktion Prozesse): im Anhang

## 7.8 Kommunikation:

- Nach den direkten Verantwortlichen, wenn nötig sollten die restlichen Mieter*innen im Zentrum informiert werden und dann, die Polizei
- Mitarbeiter*innen sollten so informiert werden, dass sie bei der Eindämmung des Problems helfen können, oder es zumindest vermeiden können.
- Mieter*innen sollten je nach Art des Angriffs entweder im Detail informiert werden oder nur in Kenntnis gesetzt werden. Dies hängt davon ab wie groß die angegriffene Fläche ist und ob sie selbst akut betroffen sind.

## 7.9 Rechtliche Bedenken

Nach manchen Vorfällen gibt es keine technische Behebungsmöglichkeit und es sind stattdessen rechtliche Schritte erforderlich.

### 7.9.1 Identitätsdiebstahl

- Polizei informieren
- Beweise sichern (Screenshots, Emails)

### 7.9.2 Offenlegung privater Information / Schutz der Privatsphäre (Doxxing)

- Betroffene Daten, wenn möglich ändern.
- Digitalen Footprint verkleinern: Social Media Accounts privat stellen, Verknüpfbarkeit mit persönlichen Daten vermeiden.

### 7.9.3 Mobbing und Cyberstalking

- Kontakt abbrechen und Polizei informieren.
- Beweise sichern Beispiele (Screenshots, Emails)
- Sicherheitseinstellungen überprüfen und Passwörter ändern

# Kindl Areal Gelände

## Fahrräder auf öffentlichen Flächen

Um Fahrraddiebstahl auf öffentlichen Flächen zu minimieren, sollte ein hochwertiges Schloss verwendet werden, wie z. B. ein U-Schloss oder ein Kettenschloss aus gehärtetem Stahl. Beim Abstellen des Fahrrads ist es wichtig, das Schloss durch den Rahmen und ein festes, unbewegliches Objekt zu führen, um das Fahrrad bestmöglich zu sichern.

Aufgrund der öffentlichen Lage des Abstellplatzes und der bereits bekannten Diebstahlsfälle in der Umgebung ist es ratsam, immer zwei verschiedene Schlösser zu verwenden – zum Beispiel ein U-Schloss für den Rahmen und ein Kettenschloss für das Vorderrad oder andere Teile des Fahrrads. Diese Doppelabsicherung erschwert den Diebstahl erheblich, da Diebe häufig nur eine Art von Schloss in der Lage sind zu knacken.