**Meldung von**

**Sicherheitsvorfällen**PINK GmbH Thermosysteme
Internal Document

**Erstellung**:
Johannes Freiburg
07.04.2025

**Freigabe:**
Philipp Hartdegen
07.04.025

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Datum | Autor | Beschreibung |
| 1.0 | 07.04.2025 | Johannes Freiburg | Erstellung des Dokuments |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Klassifizierung

Dieses Dokument ist mit einer Klassifizierung versehen. Die Kennzeichnung ist auf dem Titelblatt unter der Überschrift einzusehen.

Unsere Organisation unterscheidet die folgenden Stufen der Informationsklassifizierung für die Vertraulichkeit, bis auf Stufe 4 Sensitive, da wir Daten dieser Klassifizierung weder erheben noch speichern:

* Public
* Internal
* Confidential

**Public**
Informationen dieser Art können frei an jedermann verteilt werden.

**Internal**Informationen dieser Art sollen intern aufbewahrt werden, aber es wäre nicht schädlich, wenn sie in falsche Hände geraten würden. Diese Informationen können mit allen Stakeholdern geteilt werden, wenn dies als notwendig erachtet wird.

**Confidential**Der Verlust vertraulicher Informationen kann eine Bedrohung für die Organisation darstellen.

Die genannten Klassifizierungen unterscheiden sich im Dokumentenumgang wie folgt:

|  |  |  |  |
| --- | --- | --- | --- |
| Klassifizierung | Transport | Speicherung | Löschung |
| Public | Keine Einschränkungen, keine speziellen Sicherheitsmaßnahmen erforderlich | In allgemein zugänglichen Systemen und Ordnern, ohne besondere Schutzmaßnahmen | Einfaches Löschen, durch Verschieben in den Papierkorb und anschließendes Leeren |
| Internal | Innerhalb der Organisation oder an autorisierte externe Partner, durch: E-Mail, Transferordner, Telefon, Download, interne tragbare Medien | In zugriffsgeschützten Systemen und Ordnern, für autorisierte Benutzer  | Sicheres Löschen, z.B. durch Überschreiben der Daten oder spezielle Löschsoftware |
| Confidential | Verschlüsselt und zusätzlich durch einen 2. Faktor geschützt | In zugriffsgeschützten Systemen und Ordnern, physische Sicherheitsmaßnahmen für analoge Daten | Sicher und endgültig, z.B. durch physische Zerstörung von Datenträgern oder spezielle Löschsoftware |

**Meldung von Sicherheitsvorfällen**

**Zweck**

Dieses Dokument beschreibt das Verfahren zur Meldung von. Es soll sicherstellen, dass alle relevanten Parteien wissen, wie sie Vorfälle melden können und welche Schritte danach folgen.

**Meldeverfahren**

**E-Mail:** Senden Sie eine detaillierte Beschreibung des Vorfalls an isb@pink.de.

**Telefon:** Rufen Sie unseren Informationssicherheitsbeauftragten unter +49 (0) 93 42 / 919-233 an.

**Informationen zur Meldung**

Bitte stellen Sie folgende Informationen bereit:

* Datum und Uhrzeit des Vorfalls
* Beschreibung des Vorfalls
* Betroffene Systeme oder Daten
* Kontaktinformationen des Meldenden
* Schweregrad des Vorfalls: Einschätzung, ob der Vorfall als Störung, Notfall oder Krise eingestuft wird (wobei Telefon für dringende Fälle genutzt werden kann).
* Ergriffene Sofortmaßnahmen: Beschreibung der Maßnahmen, die bereits ergriffen wurden, um den Vorfall zu beheben oder einzudämmen.

**Beispiele für Vorfälle der Informationssicherheit:**

Fehlfunktion einer Sicherheitsmaßnahme (z.B. eines Schlosses oder Alarms)

Fehlfunktion von Hardware oder Software

Datenleck/unberechtigte Zugriffe auf Daten oder Verletzungen der Vertraulichkeit

Verstoß gegen Richtlinien oder Anweisungen

Zugangsverletzungen zu Daten/Informationen/Werten

Phishing-Angriffe: Versuche, sensible Informationen wie Passwörter oder Kreditkartendaten durch gefälschte E-Mails oder Websites zu erlangen.

Malware-Infektionen: Infektion von Systemen durch Schadsoftware wie Viren, Trojaner oder Ransomware.

Denial-of-Service (DoS) Angriffe: Angriffe, die darauf abzielen, Systeme oder Netzwerke durch Überlastung unzugänglich zu machen.

Verlust oder Diebstahl von Geräten: Verlust oder Diebstahl von Laptops, Smartphones oder anderen Geräten, die sensible Daten enthalten.

Unbefugter Zugriff: Unbefugter Zugriff auf Systeme, Netzwerke oder Daten durch interne oder externe Parteien.

Verletzung der Datensicherheit: Unbeabsichtigte Offenlegung oder Verlust von vertraulichen Informationen.

**Reaktionszeiten**

Eingangsbestätigung: Innerhalb von 24 Stunden nach Eingang der Meldung.

Analyse und Bewertung: Innerhalb von 48 Stunden nach Eingang der Meldung.

Rückmeldung: Nach erfolgreicher Beseitigung des Vorfalls über die Ergebnisse und gegebenenfalls eingeleitete Maßnahmen.

**Kontaktinformationen des ISB**

Name: Johannes Freiburg

E-Mail: jfreiburg@pink.de

Telefon: +49 (0) 93 42 / 919-233

Adresse: PINK GmbH Thermosysteme, Am Kessler 6, 97877 Wertheim, Germany