Informations-sicherheitsrichtlinie

Zweck und Geltungsbereich

Diese Informationssicherheitsrichtlinie (ISR) definiert die Grundsätze, Maßnahmen und Verfahren zur Sicherstellung der Informationssicherheit gemäß Anforderungen des ISA Kataloges von enx® sowie der ISO 27001. Sie gilt für alle Mitarbeitenden, Auftragnehmenden, Partner und Dritte, die Zugang zu den Informationen und Informationssystemen unseres Unternehmens haben.

Verantwortlichkeiten

Geschäftsführung

Verantwortlich für die Festlegung und Genehmigung der ISR.

Bereitstellung der notwendigen personellen und finanziellen Ressourcen zur Umsetzung der ISR.

Festlegung von Informationssicherheitsstrategien.

Informationssicherheitsbeauftragte (ISB)

Umsetzung und Überwachung der ISR.

Durchführung regelmäßiger Schulungen und Sensibilisierungen zur Informationssicherheit.

Durchführung und Koordination von Informationssicherheitsaudits und -bewertungen.

Überprüfung und Aktualisierung der ISR in regelmäßigen Abständen (1x jährlich und bei groben Änderungen).

Abteilungsleitende

Sicherstellung der Umsetzung der ISR in ihren jeweiligen Abteilungen.

Unterstützung der ISB bei der Durchführung von Sicherheitsmaßnahmen.

Förderung einer Sicherheitskultur innerhalb der Abteilungen.

Mitarbeitende

Einhaltung der ISR und Teilnahme an Schulungen zur Informationssicherheit.

Melden von sicherheitsrelevanten Vorfällen über die Meldewege:

a) Via Mail an IT und VJE
b) Via Incident Report Button im AIRSKIN Monitor
c) Per Telefon an die ISB

Fristgerechte Absolvierung der Online-Schulung

Vertraulicher Umgang mit Unternehmensinformationen.

Informationsklassifizierung

Klassifizierung

Informationen werden nach 3 Schutzzielen (Integrität, Vertraulichkeit und Verfügbarkeit) bewertet. Aus dieser Bewertung ergibt sich der Schutzbedarf. Informationswerte und -träger werden dementsprechend in der Assetliste gekennzeichnet.

Kategorien von Informationen

- Kategorie 1 – Keine sensiblen Informationen

  Informationen die keinen Wert für die Firma bzw. Partner darstellt. z.B. allgemeine Internetrecherche. Informationen die allgemein bekannt oder öffentlich verfügbar sind.

- Kategorie 2 – Vertrauliche Informationen

  Informationen die von höherer Bedeutung für die Firma und Partner sind. Z.B. Geschäftsprozesse deren Leak keine schwerwiegenden Folgen für uns als Firma hat

- Kategorie 3 – Geschützte Informationen

  Informationen die z.B. durch eine NDA mit einem Partner geschützt sind und deren Leak schwerwiegende Folgen für uns als Firma hat.

Übertragungs- und Speicherformen

Jedwede Datenübertragung mittels USB-Sticks, die nicht von der Firmeneigenen IT ausgegeben wurden, ist untersagt.

Ferner sind für alle Datenübertragungen mit Kunden und/oder Lieferanten Sharepoint-Links zu verwenden. Unter keinen Umständen dürfen Daten als Anhang von Emails versandt werden. Dies betrifft vor allem externe Empfänger, aber auch bei internen Empfängern sind Links zu bevorzugen, da diese im Nachhinein deaktiviert werden können.

Sollte eine Datenspeicherung auf externen Festplatten oder Speichermöglichkeiten notwendig sein, ist dies im Einzelfall im IT und ISB abzustimmen.

Schutzmaßnahmen

Kategorien 2&3 sind durch starke Verschlüsselung zu schützen. Zusätzlich ist der Zugriff auf diese Informationen begrenzt lt. Benutzer*innen-Matrix (Usergruppen im AD).

Die Zustellung von Erst-Passwörtern oder Passwörtern nach dem Zurücksetzen hat durch Verschlüsselungstools wie z.B. One-Time Secret zu erfolgen.

Datenvernichtung

Sichere und vollständige Vernichtung von Informationen, die nicht mehr benötigt werden.

Erstellung und Implementierung eines Datenvernichtungsplans, der alle Arten von Datenmedien abdeckt (z.B. Papierdokumente, Festplatten, USB-Sticks, CDs/DVDs, Backup-Bänder).

Sicherstellung, dass alle Mitarbeitenden über die Richtlinien und Verfahren zur Datenvernichtung informiert und entsprechend geschult sind.

Einsatz zertifizierter Datenvernichtungsdienste für die Vernichtung von Datenmedien, die außerhalb des Unternehmens durchgeführt wird.

Methoden der Datenvernichtung

Papierdokumente: Verwendung von Aktenvernichtern, die mindestens Sicherheitsstufe P-4 (Partikelschnitt) erfüllen.

Elektronische Medien: Einsatz von Softwaretools für die sichere Datenlöschung (z.B. mehrfaches Überschreiben von Daten) oder physische Zerstörung (z.B. Schreddern, Schmelzen).

Festplatten und SSDs: Zerstörung durch zertifizierte Dienstleister oder Verwendung spezialisierter Geräte, die die Platten physisch unbrauchbar machen (z.B. Entmagnetisierung, Zerkleinerung).

Dokumentation der Datenvernichtung

Protokollierung aller Datenvernichtungsmaßnahmen einschließlich Datum, Art des Datenträgers, Methode der Vernichtung und verantwortliche Person.

Aufbewahrung der Vernichtungsprotokolle für einen definierten Zeitraum gemäß gesetzlichen und regulatorischen Anforderungen.

Zugriffskontrolle, Physiche Sichereit und Schutzzonen

Benutzerzugriff

Zugriff auf Informationssysteme wird durch ein rollenbasiertes Zugriffskontrollsystem geregelt.

Alle Benutzerkonten sind eindeutig, personalisiert und nachverfolgbar ausgelegt.

Regelmäßige Überprüfung und Aktualisierung der Benutzerrechte.

Nutzung von Zwei-Faktor-Authentifizierung (2FA) wird für alle Accounts, die über Office365 laufen, verlangt.

Sammelkonten dürfen nur im begrenzten Ausmaß und nur wenn eine Rückverfolgbarkeit nicht notwendig ist, eingesetzt werden.

Alle Benutzerinnen sind mit starken Passwörtern hinterlegt, die Richtlinien hierzu ist in den Anwendungsrichtlinien.

Physische Sicherheit und Schutzzonen

Im gesamten Unternehmen sind folgende Bereiche als Schutzzone definiert:

- Beide Serverschränke (Server und NAS)
- HR-Schrank

Zusätzlich sind sämtliche Monitore, auf die von außen oder Besucher*innen gesehen werde kann mit Bildschirmschutzfolien auszustatten.

Alle Türen sind mit bestimmten Schlüsseln aufsperrbar. Den jeweiligen Mitarbeiter*innen sind eigene Schlüsselkategorien entsprechend ihrer Datensicherheitsklasse zugeordnet.

Generelle Eingangsbereiche werden außerhalb der offiziellen Bürozeiten Video-überwacht (Liefer- und Haupteingang).

Fernzugriff

Sichere Konfiguration von VPN-Verbindungen für den Fernzugriff – vpn-Einstellungen dürfen nicht eigenhändig geändert werden.

Einsatz von Endpoint-Security-Lösungen auf mobilen Geräten und Heimarbeitsplätzen.

Incident-Management

Alle Mitarbeitenden sind verpflichtet, Sicherheitsvorfälle (Incident‘) unverzüglich an die ISB und IT zu melden

Was zählt als Incident?

Jedwedes Ereignis, das sich auf Datensicherheit auswirken könnte. Zum Beispiel sind dies Phishing Emails, versehentliche Eingabe von Zugangsdaten auf unsicher oder unseriös wirkenden Seiten, oder sonstige Vorfälle, die Zweifel hervorrufen.

Die ISB ist verantwortlich für die Einleitung der Untersuchung von Sicherheitsvorfällen, sowie die Ergreifung geeigneter Maßnahmen zur Schadensbegrenzung und Wiederherstellung des Normalbetriebs.

Die ISB stellt die Dokumentation aller Sicherheitsvorfälle und ergriffenen Maßnahmen sicher.

Schulung und Sensibilisierung

Alle Mitarbeiter*innen werden im Zuge des Onboardings auf die Informationssicherheitsagenden geschult. Weiters gibt es jährlich eine Update-Schulung sowie zusätzlich im Falle von Änderungen an der IT-Infrastruktur, die sich auf das verlangte Verhalten der Mitarbeiter*innen auswirken.

Mitarbeiter*innen werden 1x pro Jahr auf die Wichtigkeit der Informationssicherheit geschult.

Risikomanagement

Durchführung regelmäßiger (1x jährlich fix und bei Änderungen) Risikoanalysen zur Identifizierung und Bewertung von Informationssicherheitsrisiken.

Priorisierung von Maßnahmen basierend auf der Schwere und Wahrscheinlichkeit der Risiken.

Anpassung der Maßnahmenpläne basierend auf neuen Erkenntnissen und Veränderungen in der Risikolandschaft.

Datensicherung und Back-Up Erstellung

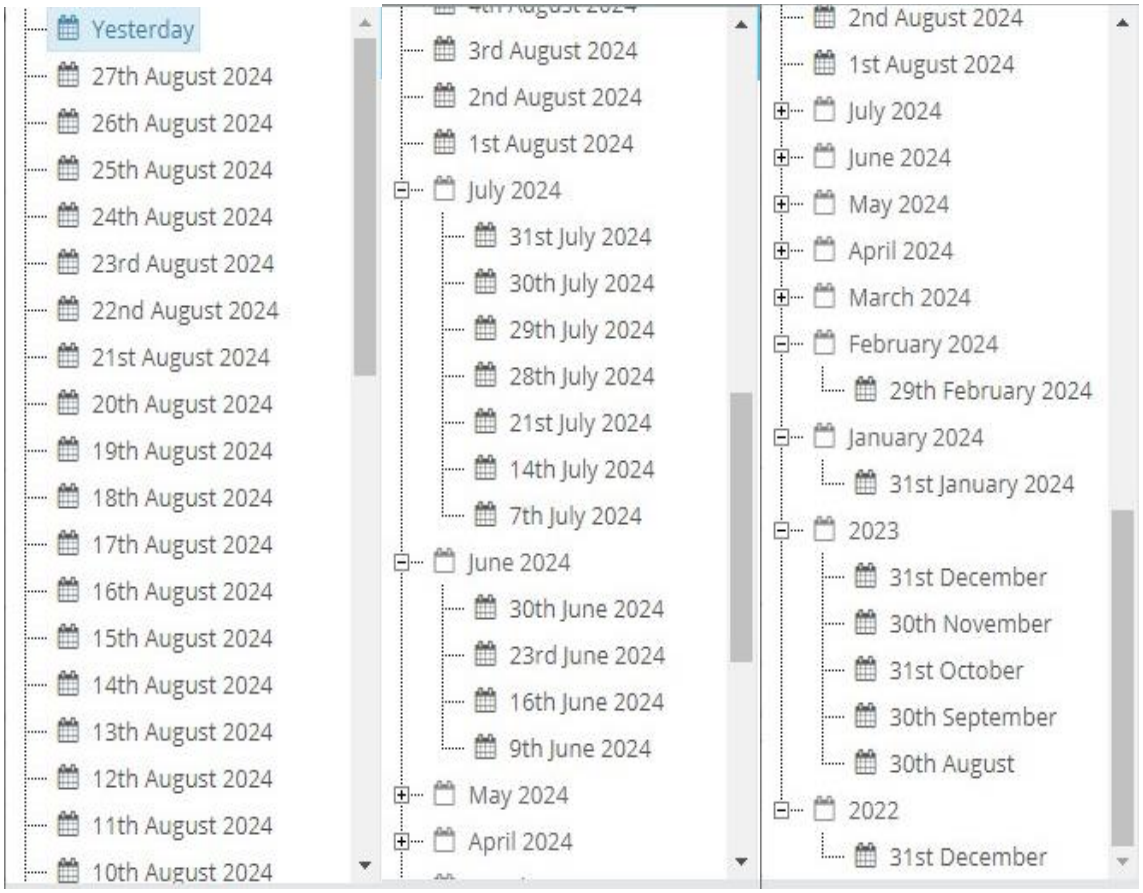
Aktuelle Backupregeln:

Unser DC01 (Domain Controller, Active Directory), der auch den Fileserver N/Z/H (interne Laufwerksbezeichnungen) enthält wird täglich um 20 Uhr an 3 Orten gesichert:

- NAS (Network Attached Server) im Serverschrank
- NAS im Verteilerschrank oben bei der Produktion
- Cloudservice in Wiener Datenzentrum

Backups werden nach einem Monat gelöscht außer:

- 1 Backup pro Woche für 12 Wochen
- 1 Backup pro Monat für 12 Monate
- 1 Backup pro Jahr für 2 Jahre



Auf unseren zweiten Server werden mit den gleichen Regeln noch folgende Virtuellen Maschinen gesichert:

- APP01
- CRM01
- DC02
- GitLab
- Nextcloud-PUBLIC
- OpenProject
- UBUNTU01-ATLASSIAN

Überprüfung und Verbesserung

- Durchführung regelmäßiger interner Audits zur Überprüfung der Einhaltung der ISR.
- Dokumentation und Setzen von Maßnahmen und Arbeiten der Audit-Ergebnisse im Ticket System.
- Identifizierung und Umsetzung von Verbesserungsmöglichkeiten basierend auf den Ergebnissen der Audits und Risikoanalysen.
- Nutzung von Feedback aus Schulungen und Vorfallberichten zur Verbesserung der Sicherheitsmaßnahmen.
- Teilnahme an externen Audits und Zertifizierungen zur Validierung der Informationssicherheitspraktiken.
- Umsetzung von Empfehlungen und Korrekturmaßnahmen aus externen Audit-Berichten.

Notfallmanagement und Wiederherstellung

Diese Punkte sind in eigenen Richtlinien genauer behandelt. BDR verfügt über einen generellen Notfallplan, einen IT-Incident spezifischen Notfallplan sowie 1 Business Continuity Concept. Zusätzlich wird der Ernstfall 1 mal jährlich mit einem Disaster Recovery Test geübt und daraus Verbesserungsmaßnahmen abgeleitet. Auch der extern durchgeführte Pen-Test gibt wertvollen Input um im Ernstfall schneller wiederhergestellt zu sein.

AIRSKIN GmbH | Niedermoserstraße 14 | 1220 Vienna, Austria | +43 1 890 86 97
office@airskin.io | FN 633792y| Handelsgericht St. Pölten | UID ATU81128824