Technisch Organisatorische Maßnahmen

ÖWD cleaning services GmbH & Co KG
Bayerhamerstr. 14c
5020 Salzburg
Österreich

1. Zutrittskontrolle

Absicherung von Eingängen, Fenstern, Serverraum, etc.

Beschreibung:

Speziell das Herzstück das NSC ist besonders gut gesichert und erfüllt die ÖVE/ÖNORM EN 50518-1.
Die Norm beinhaltet unter anderem örtliche und bauliche Anforderungen wie Anforderung gegen Angriffe mit Schusswaffen, Anforderung gegen Feuer, Anforderung gegen Blitzschlag, Regelungen zur Personenschleuse, Lüftung und vieles mehr.
Der Wiederstand von Türen, und verglasten Bereichen des NSC muss die Anforderungen von EN 1627, Wiederstandsklasse 3 (WK 3/en: RC3) erfüllen.
Türen und verglaste Bereiche des NSC erfüllen die Anforderungen der EN 1522, FB3 gegen Angriffe mit Schusswaffen.
Die Außenhaut des NSC bietet einen Feuerwiederstand entsprechend EN 13501-2, aber nicht weniger als 30 min.

Risiken:

Zutritt von Unbefugten, Diebstahl

Alarmanlage

Beschreibung:

Alarmanlagen des NSC:
Es sind elektronische Erkennungen für alle wesentlichen Teile des NSC wie folgt vorhanden:
- externe Angreifer (Einbruchmeldeanlage nach EN50131-1 Sicherheitsgrad 3);
- Feuer (EN 54 / EN 54-14);
- Zutritt/Austritt (Personenschleuse);
- Gas (Gasmeldeanlage mindestens Kohlenmonoxid);
- Kommunikation (Störungserkennung EN 50136-1);
- Überfall (Überfallmelder nach EN 50131-1);
- Überwachungsmaßnahmen zum Schutz des Personals (min alle 60min);
- Meldungen von den elektronischen Schutzanlagen;
- Videoüberwachung (EN 50132-7);

Alle Anlagen werden in Übereinstimmung mit den maßgeblichen Normen instandgehalten. Dort wo keine Normen vorhanden sind, erfolgt die Instandhaltung in Übereinstimmung mit den Hersteller-Vorgaben um die Funktionssicherheit zu jeder Zeit sicherzustellen.

Risiken:

Zutritt von Unbefugten, Diebstahl

Automatisches Zugangskontrollsystem

Beschreibung:

Eine zuverlässige Zutrittskontrolle zu Unternehmensgelände und Firmenräumlichkeiten ist die Basis des modernen Sicherheitskonzepts des ÖWD. Mit einer Unternehmensweiten Zutrittskontrolle wird entschieden, wer, wann zu welchen Bereichen Zutritt erhält. Über die Hauseigene Zutrittssoftware Sphinx besteht dabei jederzeit Einblick in den aktuellen Zutrittsstatus. Selbstverständlich werden auch unberechtigte Zutrittsversuche dokumentiert, um Unregelmäßigkeiten rechtzeitig feststellen zu können.

Risiken:

Zutritt von Unbefugten

Chipkarten-/Transponder-Schließsystem

Beschreibung:
Der Zugang zu den Unternehmensgebäuden, Stockwerken sowie sensiblen Räumlichkeiten des Unternehmens ist über elektronische Chip-Schließsysteme geregelt.

Risiken:
Zutritt von Unbefugten

Manuelles Schließsystem

Beschreibung:
Manuelle Schließsystem sind als ergänzende Sicherheitsstufe zu elektronischen, automatischen Schließsystem im Einsatz und erhöhen so das Sicherheitslevel zusätzlich.

Risiken:
Zutritt von Unbefugten

Personenkontrolle beim Pförtner / Empfang

Beschreibung:
Die Zentrale in Salzburg verfügt über einen 24/7 Portierdienst. Außerhalb der Geschäftszeiten wird diese Aufgabe von der Einsatzzentrale übernommen.

Das NSC Wien ist 24/7 besetzt, alle Besucher müssen sich in ein Besucherbuch eintragen.
Das NSC verfügt darüber hinaus über eine Personenschleuse mit gegenseitig verriegelten Türen welche nicht gleichzeitig geöffnet werden können. Die Türen der Schleuse sind mit automatisch selbstschließenden Verschluss- und Entriegelungseinrichtungen ausgestattet, welche ausschließlich von innerhalb des NSC bedient werden können.

Risiken:
Zutritt von Unbefugten

Protokollierung der Besucher

Beschreibung:
Die Zentrale in Salzburg verfügt über einen 24/7 Portierdienst. Außerhalb der Geschäftszeiten wird diese Aufgabe von der Einsatzzentrale übernommen.

Das NSC Wien ist 24/7 besetzt, alle Besucher müssen sich in ein Besucherbuch eintragen.
Das NSC verfügt darüber hinaus über eine Personenschleuse mit gegenseitig verriegelten Türen welche nicht gleichzeitig geöffnet werden können. Die Türen der Schleuse sind mit automatisch selbstschließenden Verschluss- und Entriegelungseinrichtungen ausgestattet, welche ausschließlich von innerhalb des NSC bedient werden können.

Risiken:
Zutritt von Unbefugten

Schlüsselregelung (Schlüsselausgabe etc.)

Beschreibung:
Das ÖWD-Schlüsselmanagement ist eine der Kerntätigkeiten des ÖWD. Das ÖWD-Schlüsselmanagement sorgt dafür, dass der hinterlegte Schlüssel einer berechtigten Person jederzeit zugänglich ist. Auf Wunsch werden die Schlüssel auch zum Objekt gebracht. Bei der Schlüsselaufbewahrung werden Aus- und Rückgabe dokumentiert.

Risiken:
Zutritt von Unbefugten

Sicherheitsschlösser

Beschreibung:
Verschlusseinrichtungen des NSC:
Es befinden sich elektromechanische Schließeinrichtungen nach EN 14846 in der Klasse 2-R-2-B-0-C-7-H-B-3-E-4-3 (siehe ÖVE/ÖNORM EN 50518-1 A.1 für die Anforderung an den Schlosscode) im Einsatz um die Türen der Personenschleuse zu sichern. Die Befestigungsschrauben sind im geschlossenen Zustand der Türen gegen Sabotage geschützt. Eine mechanische Freischaltung zur Notbefreiung ist vorhanden und gegen unbeabsichtigte Betätigung gesichert.
Andere Türen sind mittels mechanischen Schließeinrichtungen in Übereinstimmung mit EN 12209, Klasse 2-R-2-1-0-C-7-H-B-3-E (siehe ÖVE/ÖNORM EN 50518-1 A.2 für die Anforderung an den Schlosscode) gesichert.

Risiken:
Zutritt von Unbefugten, Diebstahl

Sorgfältige Auswahl von Reinigungspersonal

Beschreibung:
Die Auswahl vertrauenswürdiger Mitarbeiter ist Kerngeschäft des Verantwortlichen und in der Gewebeordnung verankert. Selbstverständlich muss auch das Reinigungspersonal diesen hohen Anforderungen genügen.

§ 130 GewO 1994 Rechte und Pflichten der Berufsdetektive und Bewacher

(3) Gewerbetreibende, die zur Ausübung des Bewachungsgewerbes berechtigt sind, sind auch zur Fahrzeug- und Transportbegleitung berechtigt.
...
(8) Die zur Ausübung des Gewerbes der Berufsdetektive sowie die zur Ausübung des Bewachungsgewerbes berechtigten Gewerbetreibenden dürfen zur Ausübung der ihren Gewerben vorbehaltenen Tätigkeiten (§ 129 Abs. 1 bzw. Abs. 4) nur Arbeitnehmer verwenden, die eigenberechtigt sind und die für diese Verwendung erforderliche Zuverlässigkeit und Eignung besitzen.
(9) Die im Abs. 8 genannten Gewerbetreibenden sind verpflichtet, der Bezirksverwaltungsbehörde, im Gebiet einer Gemeinde, für das die Landespolizeidirektion zugleich Sicherheitsbehörde erster Instanz ist, der Landespolizeidirektion, als Sicherheitsbehörde ein Verzeichnis aller Personen, die für eine der im § 129 Abs. 1 bzw. Abs. 4 genannten Tätigkeiten herangezogen werden, spätestens zwei Wochen vor dem Beginn ihrer Verwendung vorzulegen; jede Änderung hinsichtlich der für die im § 129 Abs. 1 bzw. Abs. 4 genannten Tätigkeiten herangezogenen Personen ist dieser Behörde binnen zwei Wochen anzuzeigen. Das Verzeichnis oder die Anzeigen von Änderungen dieses Verzeichnisses haben neben dem Vor- und Familiennamen der betreffenden Person auch deren Geburtsdatum, Geburtsort, Staatsangehörigkeit und Unterkunft (Wohnung) zu enthalten.
(10) Ist auf Grund bestimmter Tatsachen die Zuverlässigkeit einer gemäß Abs. 9 bekannt gegebenen Person nicht gegeben, so hat die Sicherheitsbehörde dem Gewerbetreibenden ohne unnötigen Aufschub schriftlich mitzuteilen, dass der Betroffene die erforderliche Zuverlässigkeit nicht besitzt.

Risiken:
Zutritt von Unbefugten

Sorgfältige Auswahl von Wachpersonal

Beschreibung:
Die Auswahl vertrauenswürdiger Mitarbeiter ist Kerngeschäft des ÖWD und in der Gewebeordnung verankert.

§ 130 GewO 1994 Rechte und Pflichten der Berufsdetektive und Bewacher

(3) Gewerbetreibende, die zur Ausübung des Bewachungsgewerbes berechtigt sind, sind auch zur Fahrzeug- und Transportbegleitung berechtigt.
...
(8) Die zur Ausübung des Gewerbes der Berufsdetektive sowie die zur Ausübung des Bewachungsgewerbes berechtigten Gewerbetreibenden dürfen zur Ausübung der ihren Gewerben vorbehaltenen Tätigkeiten (§ 129 Abs. 1 bzw. Abs. 4) nur Arbeitnehmer verwenden, die eigenberechtigt sind und die für diese Verwendung erforderliche Zuverlässigkeit und Eignung besitzen.
(9) Die im Abs. 8 genannten Gewerbetreibenden sind verpflichtet, der Bezirksverwaltungsbehörde, im Gebiet einer Gemeinde, für das die Landespolizeidirektion zugleich Sicherheitsbehörde erster Instanz ist, der Landespolizeidirektion, als Sicherheitsbehörde ein Verzeichnis aller Personen, die für eine der im § 129 Abs. 1 bzw. Abs. 4 genannten Tätigkeiten herangezogen werden, spätestens zwei Wochen vor dem Beginn ihrer Verwendung vorzulegen; jede Änderung hinsichtlich der für die im § 129 Abs. 1 bzw. Abs. 4 genannten Tätigkeiten herangezogenen Personen ist dieser Behörde binnen zwei Wochen anzuzeigen. Das Verzeichnis oder die Anzeigen von Änderungen dieses Verzeichnisses haben neben dem Vor- und Familiennamen der betreffenden Person auch deren Geburtsdatum, Geburtsort, Staatsangehörigkeit und Unterkunft (Wohnung) zu enthalten.
(10) Ist auf Grund bestimmter Tatsachen die Zuverlässigkeit einer gemäß Abs. 9 bekannt gegebenen Person nicht gegeben, so hat die Sicherheitsbehörde dem Gewerbetreibenden ohne unnötigen Aufschub schriftlich mitzuteilen, dass der Betroffene die erforderliche Zuverlässigkeit nicht besitzt.

Risiken:
Zutritt von Unbefugten

Videoüberwachung der Zugänge

Beschreibung:
Videoüberwachung des NSC:
CCTV-Überwachung nach EN 50518-1
Innerhalb der NEC ist eine Überwachungsmöglichkeit vorhanden, so dass alle Annäherungen zum Gebäude, in dem das NSC untergebracht ist, nach den Anwendungsrichtlinien der EN 50132-7 von innen überwacht werden können.
Es ist eine Überwachungsmöglichkeit vorhanden, die es dem NSC-Personal ermöglicht, berechtigte Personen zu erkennen, bevor es ihnen den Zutritt in die Personenschleuse des NSC ermöglicht.

Risiken:
Zutritt von Unbefugten

2. Zugangskontrolle

Einsatz einer Hardware-Firewall

Beschreibung:

Die redundant ausgelegte Firewall schottet das interne Netzwerk (LAN oder Intranet) vom restlichen Netzwerk (insbesondere vom globalen Internet) ab. Regelmäßige Wartungen und Überprüfungen gewähren Aktualität und erhöhen die IT Sicherheit.

Auszug aus der ÖWD Leitlinie zur Informationssicherheit:
"Computer-Viren-Schutzprogramme werden auf allen IT-Systemen eingesetzt. Alle Internetzugänge werden durch eine geeignete Firewall gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Des Weiteren unterstützen die IT-Benutzer durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten die entsprechend festgelegten Stellen."

Risiken:

Hacking

Einsatz einer Software-Firewall

Beschreibung:

Auf sämtlichen Rechnern und Servern ist ein Virenschutz mit integrierter personal Firewall installiert. Der Virenschutz wird zentral verwaltet und ermöglicht somit maximale Kontrolle auf Aktualität und Aktivität des Virenscanners.

Auszug aus der ÖWD Leitlinie zur Informationssicherheit:
"Computer-Viren-Schutzprogramme werden auf allen IT-Systemen eingesetzt. Alle Internetzugänge werden durch eine geeignete Firewall gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Des Weiteren unterstützen die IT-Benutzer durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten die entsprechend festgelegten Stellen."

Risiken:

Hacking

Einsatz von Anti-Viren-Software

Beschreibung:

Auf sämtlichen Rechnern und Servern ist ein Virenschutz mit integrierter personal Firewall installiert. Der Virenschutz wird zentral verwaltet und ermöglicht somit maximale Kontrolle auf Aktualität und Aktivität des Virenscanners.

Auszug aus der ÖWD Leitlinie zur Informationssicherheit:
"Computer-Viren-Schutzprogramme werden auf allen IT-Systemen eingesetzt. Alle Internetzugänge werden durch eine geeignete Firewall gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Des Weiteren unterstützen die IT-Benutzer durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten die entsprechend festgelegten Stellen."

Risiken:

Hacking, Trojaner, Viren, Ransomware

Einsatz von VPN-Technologie

Beschreibung:
Alle Filialen sind via LIC+ Leitungen angebunden und bilden das interne Firmennetzwerk. Den Zugriff auf das Firmennetzwerk von außen regelt eine redundant ausgelegte Firewall, welche auch ein VPN Gateway bereitstellt. Firmenlaptops ist es so möglich sich via VPN-Tunnel auch von außen sicher mit dem Firmennetzwerk zu verbinden.

Risiken:
Nutzung von Unbefugten, Hacking

Erstellen von Benutzerprofilen

Beschreibung:
Benutzerprofile werden ausschließlich unter dem vier Augenprinzip angelegt.

Risiken:
Nutzung von Unbefugten

Passwortvergabe

Beschreibung:
Die Vergabe der Passwörter erfolgt unter Berücksichtigung der Passwortrichtlinie. Die User sind angehalten das Passwort nach Erhalt umgehend in ein nur ihnen bekanntes Passwort zu ändern.

Risiken:
Nutzung von Unbefugten

Verhaltensregeln:
Die Passwortrichtlinie ist Teil der ÖWD IT-Richtlinie (Absatz 4.6. Kennwortschutz):
§20 Alle Kennwörter müssen folgende Voraussetzungen erfüllen:
- Das Kennwort darf nicht den Kontonamen des Benutzers oder mehr als zwei Zeichen enthalten, die nacheinander im vollständigen Namen des Benutzers vorkommen.
- Jedes Passwort darf nicht länger als 60 Tage verwendet werden.
- Das Kennwort muss mindestens sechs Zeichen lang sein.
- Das Kennwort muss Zeichen aus drei der folgenden Kategorien enthalten:
  - Großbuchstaben (A bis Z)
  - Kleinbuchstaben (a bis z)
  - Zahlen zur Basis 10 (0 bis 9)
  - Nicht alphabetische Zeichen (zum Beispiel: !, $, #, %)

§21 Jeder Rechner muss sich nach maximal 15 Minuten Untätigkeit automatisch in den Sperrzustand versetzen und bei Reaktivierung ein Kennwort verlangen. Für Telefone und Tablets gilt eine maximale Dauer von einer Minute Untätigkeit.
§22 Die Weitergabe oder unverschlüsselte Aufbewahrung der Passwörter von persönlichen Zugängen ist untersagt!

Personenkontrolle beim Pförtner / Empfang

Beschreibung:
Die Zentrale in Salzburg verfügt über einen 24/7 Portierdienst. Außerhalb der Geschäftszeiten wird diese Aufgabe von der Einsatzzentrale übernommen.
Die NSC Wien ist ebenfalls 24/7 besetzt und Besucher müssen sich in ein Besucherbuch eintragen.

Risiken:
Nutzung von Unbefugten

Protokollierung der Besucher

Beschreibung:
Alle Besucher des NSC müssen sich in ein Besucherbuch eintragen.

Risiken:
Nutzung von Unbefugten

Schlüsselregelung (Schlüsselausgabe etc.)

Beschreibung:
Das ÖWD-Schlüsselmanagement ist eine der Kerntätigkeiten des ÖWD. Das ÖWD-Schlüsselmanagement sorgt dafür, dass der hinterlegte Schlüssel einer berechtigten Person jederzeit zugänglich ist. Auf Wunsch werden die Schlüssel auch zum Objekt gebracht. Bei der Schlüsselaufbewahrung werden Aus- und Rückgabe dokumentiert.

Risiken:
Nutzung von Unbefugten

Sicherheitsschlösser

Beschreibung:
Verschlusseinrichtungen des NSC:
Es befinden sich elektromechanische Schließeinrichtungen nach EN 14846 in der Klasse 2-R-2-B-0-C-7-H-B-3-E-4-3 (siehe ÖVE/ÖNORM EN 50518-1 A.1 für die Anforderung an den Schlosscode) im Einsatz um die Türen der Personenschleuse zu sichern. Die Befestigungsschrauben sind im geschlossenen Zustand der Türen gegen Sabotage geschützt. Eine mechanische Freischaltung zur Notbefreiung ist vorhanden und gegen unbeabsichtigte Betätigung gesichert.
Andere Türen sind mittels mechanischen Schließeinrichtungen in Übereinstimmung mit EN 12209, Klasse 2-R-2-1-0-C-7-H-B-3-E (siehe ÖVE/ÖNORM EN 50518-1 A.2 für die Anforderung an den Schlosscode) gesichert.

Risiken:
Nutzung von Unbefugten

Sorgfältige Auswahl von Reinigungspersonal

Beschreibung:
Die Auswahl vertrauenswürdiger Mitarbeiter ist Kerngeschäft des ÖWD und in der Gewebeordnung verankert. Selbstverständlich muss auch das Reinigungspersonal diesen hohen Anforderungen genügen.

§ 130 GewO 1994 Rechte und Pflichten der Berufsdetektive und Bewacher

(3) Gewerbetreibende, die zur Ausübung des Bewachungsgewerbes berechtigt sind, sind auch zur Fahrzeug- und Transportbegleitung berechtigt.
...
(8) Die zur Ausübung des Gewerbes der Berufsdetektive sowie die zur Ausübung des Bewachungsgewerbes berechtigten Gewerbetreibenden dürfen zur Ausübung der ihren Gewerben vorbehaltenen Tätigkeiten (§ 129 Abs. 1 bzw. Abs. 4) nur Arbeitnehmer verwenden, die eigenberechtigt sind und die für diese Verwendung erforderliche Zuverlässigkeit und Eignung besitzen.
(9) Die im Abs. 8 genannten Gewerbetreibenden sind verpflichtet, der Bezirksverwaltungsbehörde, im Gebiet einer Gemeinde, für das die Landespolizeidirektion zugleich Sicherheitsbehörde erster Instanz ist, der Landespolizeidirektion, als Sicherheitsbehörde ein Verzeichnis aller Personen, die für eine der im § 129 Abs. 1 bzw. Abs. 4 genannten Tätigkeiten herangezogen werden, spätestens zwei Wochen vor dem Beginn ihrer Verwendung vorzulegen; jede Änderung hinsichtlich der für die im §

129 Abs. 1 bzw. Abs. 4 genannten Tätigkeiten herangezogenen Personen ist dieser Behörde binnen zwei Wochen anzuzeigen. Das Verzeichnis oder die Anzeigen von Änderungen dieses Verzeichnisses haben neben dem Vor- und Familiennamen der betreffenden Person auch deren Geburtsdatum, Geburtsort, Staatsangehörigkeit und Unterkunft (Wohnung) zu enthalten.
(10) Ist auf Grund bestimmter Tatsachen die Zuverlässigkeit einer gemäß Abs. 9 bekannt gegebenen Person nicht gegeben, so hat die Sicherheitsbehörde dem Gewerbetreibenden ohne unnötigen Aufschub schriftlich mitzuteilen, dass der Betroffene die erforderliche Zuverlässigkeit nicht besitzt.

Risiken:
Nutzung von Unbefugten

Sorgfältige Auswahl von Wachpersonal

Beschreibung:
§ 130 GewO 1994 Rechte und Pflichten der Berufsdetektive und Bewacher

(3) Gewerbetreibende, die zur Ausübung des Bewachungsgewerbes berechtigt sind, sind auch zur Fahrzeug- und Transportbegleitung berechtigt.
...
(8) Die zur Ausübung des Gewerbes der Berufsdetektive sowie die zur Ausübung des Bewachungsgewerbes berechtigten Gewerbetreibenden dürfen zur Ausübung der ihren Gewerben vorbehaltenen Tätigkeiten (§ 129 Abs. 1 bzw. Abs. 4) nur Arbeitnehmer verwenden, die eigenberechtigt sind und die für diese Verwendung erforderliche Zuverlässigkeit und Eignung besitzen.
(9) Die im Abs. 8 genannten Gewerbetreibenden sind verpflichtet, der Bezirksverwaltungsbehörde, im Gebiet einer Gemeinde, für das die Landespolizeidirektion zugleich Sicherheitsbehörde erster Instanz ist, der Landespolizeidirektion, als Sicherheitsbehörde ein Verzeichnis aller Personen, die für eine der im § 129 Abs. 1 bzw. Abs. 4 genannten Tätigkeiten herangezogen werden, spätestens zwei Wochen vor dem Beginn ihrer Verwendung vorzulegen; jede Änderung hinsichtlich der für die im § 129 Abs. 1 bzw. Abs. 4 genannten Tätigkeiten herangezogenen Personen ist dieser Behörde binnen zwei Wochen anzuzeigen. Das Verzeichnis oder die Anzeigen von Änderungen dieses Verzeichnisses haben neben dem Vor- und Familiennamen der betreffenden Person auch deren Geburtsdatum, Geburtsort, Staatsangehörigkeit und Unterkunft (Wohnung) zu enthalten.
(10) Ist auf Grund bestimmter Tatsachen die Zuverlässigkeit einer gemäß Abs. 9 bekannt gegebenen Person nicht gegeben, so hat die Sicherheitsbehörde dem Gewerbetreibenden ohne unnötigen Aufschub schriftlich mitzuteilen, dass der Betroffene die erforderliche Zuverlässigkeit nicht besitzt.

Risiken:
Nutzung von Unbefugten

Verschlüsselung von Datenträgern in Laptops / Notebooks

Beschreibung:
Alle von der IT verwalteten Unternehmenslaptops sind entweder durch TrueCrypt (ältere Geräte) oder Bitlocker verschlüsselt. Die ordnungsgemäße Verschlüsselung wird automatisiert bei Start des Gerätes im Unternehmensnetzwerk überprüft und etwaige Abweichungen gemeldet.

Risiken:
Nutzung von Unbefugten bei Verlust

Verschlüsselung von mobilen Datenträgern

Beschreibung:
Die Mitarbeiter sind laut IT Richtlinie dazu verpflichtet alle mobilen Datenträger auf denen sich Unternehmensdaten befinden zu verschlüsseln.

Risiken:
Nutzung von Unbefugten bei Verlust

Verschlüsselung von Smartphone-Inhalten

Beschreibung:

Mobile Device Policy
§17. Alle Geräte, sofern technisch möglich, müssen verschlüsselt werden.

Risiken:

Nutzung von Unbefugten bei Verlust

Zuordnung von Benutzerprofilen zu IT-Systemen

Beschreibung:

Die Zuordnung der Benutzerprofile zu den IT-Systemen erfolgt unter dem vier Augen Prinzip. Soweit möglich erfolgt die Anmeldung an den IT-Systemen dann über SSo (Single Sign on) was nicht nur eine Zeitersparnis darstellt, da nur noch eine einzige Authentifizierung notwendig ist, sondern auch einen Sicherheitsgewinn darstellt, da das Passwort nur einmal übertragen werden muss und da sich der Nutzer anstelle einer Vielzahl meist unsicherer Passwörter nur noch eines merken muss, somit kann dieses eine Passwort dafür komplex und sicher gewählt werden. Auch Phishing-Attacken werden erschwert, da Benutzer UserID und Passwort nur an einer einzigen Stelle eingeben müssen und nicht mehr an zahlreichen, verstreuten Stellen. Diese eine Stelle kann leichter auf Korrektheit (URL, SSL-Serverzertifikat, etc.) überprüft werden.

Risiken:

Nutzung von Unbefugten

Zuordnung von Benutzerrechten

Beschreibung:

Die Zuordnung der Benutzerrechte erfolgt nach dem vier Augen Prinzip.

Auszug aus der ÖWD Leitlinie zur Informationssicherheit:
"Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme ist eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen vergibt. Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass Vertreter ihre Aufgaben erfüllen können."

Risiken:

Nutzung von Unbefugten

3. Zugriffskontrolle

Anzahl der Administratoren auf das „Notwendigste“ reduziert

Beschreibung:
Die Anzahl der Administratoren ist bewusst klein gehalten. Jeder Administrator hat genau die Rechte, welche benötigt werden, um die definierten Aufgaben zu erfüllen.

Risiken:
Datenzugriff von Unbefugten

Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

Beschreibung:
Ein Abfallwirtschaftskonzept pro Standort wurde erstellt und ein Abfallbeauftragter bestellt. Der Prozess des Abfallmanagements regelt die Vernichtung der Akten mittels Aktenvernichter oder deren zertifizierte Vernichtung durch externe Dienstleister.

Risiken:
Datenzugriff von Unbefugten

Erstellen eines Berechtigungskonzepts

Beschreibung:
Alle User werden über den Microsoft Active Directory Standard nach dem Prinzip A-G-G-P verwaltet:
A = Account
G/U = Globale Domänen Gruppe/Universelle Domänengruppe -> hier werden die User drin geclustert; z.B. alle Mitarbeiter aus Wien
G = Globale Gruppe -> diese wird zur Vergabe der Berechtigungen im Filesystem genutzt; diese Gruppe nimmt entweder die globale Gruppe oder im Ausnahmefall einzelne User auf.
P = Permission
Weiters werden die Userberechtigungen auch innerhalb der im Einsatz befindlichen Software verwaltet. Es wird stets darauf geachtet, soweit möglich, mit Berechtigungsgruppen zu arbeiten und Einzelberechtigungen weitestgehend zu vermeiden um Fehlern vorzubeugen und die Administration zu vereinfachen.
Berechtigungen werden stets nach dem vier Augen Prinzip vergeben.

Auszug aus der ÖWD Leitlinie zur Informationssicherheit:
"Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme ist eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen vergibt.
Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass Vertreter ihre Aufgaben erfüllen können."

Risiken:
Datenzugriff von Unbefugten

Meldepflicht

Beschreibung:
Auszug aus der Mobile Device Policy:

§10. Abhanden gekommene oder gestohlene Geräte müssen der IT-Abteilung und dem

Sekretariat der GD umgehend am folgenden Werktag gemeldet werden.

§11. Vermutet ein User, dass ein unbefugter Zugriff über Mobilgeräte auf Unternehmensdaten erfolgt ist, muss er dies der IT-Abteilung in Einklang mit Melderichtlinien des ÖWD mitteilen.

ordnungsgemäße Vernichtung von Datenträgern

Beschreibung:
Alle digitalen Datenträger werden zertifiziert nach Vernichtungsstufe v5 entsorgt.

Risiken:
Datenzugriff von Unbefugten

Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

Speicherort: Cloudspeicher, Rechenzentrum (Fileserver), Mobiler Speicher (USB Stick,...), Notebook / Desktop, Mobiles Gerät (Handy, Tablet,...)

Beschreibung:
Die Passwortrichtlinie ist Teil der IT Richtlinie. Unter Punkt 4.6 "Kennwortschutz" ist der Umgang das Aussehen und die Gültigkeitsdauer von Passwörtern geregelt.

Risiken:
Datenzugriff von Unbefugten

Verhaltensregeln:
20. Alle Kennwörter müssen folgende Voraussetzungen erfüllen:
• Das Kennwort darf nicht den Kontonamen des Benutzers oder mehr als zwei Zeichen enthalten, die nacheinander im vollständigen Namen des Benutzers vorkommen.
• Jedes Passwort darf nicht länger als 60 Tage verwendet werden.
• Das Kennwort muss mindestens sechs Zeichen lang sein.
• Das Kennwort muss Zeichen aus drei der folgenden Kategorien enthalten:
- Großbuchstaben (A bis Z)
- Kleinbuchstaben (a bis z)
- Zahlen zur Basis 10 (0 bis 9)
- Nicht alphabetische Zeichen (zum Beispiel: !, $, #, %)

Ausgenommen von der Kennwortrichtlinie sind Geräte welche die technischen Voraussetzungen für die Verwendung sicherer Passwörter nicht erfüllen, wie einfache Telefone. Bei diesen Geräten ist der höchstmögliche technische Schutz zu verwenden (z.B.: vierstelliger PIN).

21. Jeder Rechner muss sich nach maximal 15 Minuten Untätigkeit automatisch in den Sperrzustand versetzen und bei Reaktivierung ein Kennwort verlangen. Für Telefone und Tablets gilt eine maximale Dauer von einer Minute Untätigkeit.

22. Die Weitergabe oder unverschlüsselte Aufbewahrung der Passwörter von persönlichen Zugängen ist untersagt!

physische Löschung von Datenträgern vor Wiederverwendung

Beschreibung:
Datenträger werden nur Unternehmensintern weiterverwendet und niemals unternehmensfremden Stellen überlassen. Alle Datenträger welche wiederverwendet werden, werden vor der Weitergabe sicher gelöscht.

Risiken:

Datenzugriff von Unbefugten

Protokollierung der Vernichtung

Beschreibung:

ISO PB_Abfallmanagement_5.00:
Alle Belege der Vernichtung werden an eine zentrale Stelle weitergeleitet. Nach abgeschlossener Erfassung werden die Belege inkl. aller Anhänge (Lieferscheine, Begleitscheine, Zertifikate, …) in Ordnern aufbewahrt.

Risiken:

Datenzugriff von Unbefugten

Sichere Aufbewahrung von Datenträgern

Beschreibung:

Auszug aus der IT Richtlinie:
§12. Das Kopieren von Dateien zum Zwecke der Heimarbeit oder zu privaten Zwecken ist strengstens untersagt!
§13. Das Abspeichern von Firmendaten auf externen Datenspeichern ist verboten! Darunter fallen auch Cloud Drives und ähnliche Technologien.
Datenträger welche für die Vernichtung gesammelt werden befinden sich in dafür vorgesehenen Behältnissen und in abgeschlossen, nur befugtem Personal zugänglichem Bereich.
Datenträger welche zum Zwecke der Sicherung gelagert werden, befinden sich in einem feuerfesten Save und in abgeschlossenem, nur befugtem Personal zugänglichem Bereich.
Datenträger welche sich im Einsatz befinden, werden permanent automatisiert überwacht und so vor Veränderung, Tausch oder Diebstal geschützt.

Risiken:

Datenzugriff von Unbefugten

Verbesserung der Sicherheit

Beschreibung:

Die Informationssicherheitsmaßnahmen werden regelmäßig auf ihre Aktualität und Wirksamkeit geprüft. Daneben werden auch die Maßnahmen regelmäßig untersucht, ob diese den betroffenen Mitarbeitern bekannt sind und ob diese umsetzbar und in den Betriebsablauf integrierbar sind.

Auszug aus der LEITLINIE ZUR INFORMATIONSSICHERHEIT DER ÖWD SECURITY & SERVICES:

Die Leitung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Mitarbeiter sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen weiterzugeben. Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheit und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der IT-Sicherheitstechnik zu halten.

Verschlüsselung von Datenträgern

Beschreibung:

Arbeitsplatzrechner sowie Laptops (Notebooks) werden seitens IT professionell und standardisiert hinsichtlich Authentisierung (User-Identifikation und Anmeldung) sowie Verschlüsselung („Bitlocker“) konfiguriert. Auch die Installation von Updates und Patches ist zentral gesteuert; individuelle Installation von Anwendungen untersagt.

Risiken:
Datenzugriff von Unbefugten bei Verlust

Verwaltung der Rechte durch Systemadministrator

Beschreibung:
Alle IT-Berechtigungen werden ausschließlich von geschulten Systemadministratoren vergeben und verwaltet.

Auszug aus der ÖWD Leitlinie zur Informationssicherheit:
"Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme ist eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen vergibt. Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass Vertreter ihre Aufgaben erfüllen können."

Risiken:
Datenzugriff von Unbefugten

Zugriff auf Firmenrechner

Beschreibung:
Auszug aus der IT-Richtlinie:
§5. Software welche internen oder externen Usern Zugriff auf Firmenrechner gibt (TeamViewer) darf nur mit Genehmigung der IT gestartet oder installiert werden.

4. Weitergabekontrolle

Beim physischen Transport: sichere Transportbehälter/-verpackungen

Beschreibung:

Der physische Transport von Gütern welche sicher und zeitgerecht von A nach B gelangen sollen ist Kerngeschäft des ÖWD. Sichere Transportbehälter und Transportverpackungen sind dabei Standard.

Risiken:

Dateneinsicht durch Dritte bei Verlust

Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen

Beschreibung:

Der physische Transport von Gütern welche sicher und zeitgerecht von A nach B gelangen sollen ist Kerngeschäft des ÖWD.
Die Auswahl vertrauenswürdiger Mitarbeiter ist in der Gewebeordnung verankert.

§ 130 GewO 1994 Rechte und Pflichten der Berufsdetektive und Bewacher

(3) Gewerbetreibende, die zur Ausübung des Bewachungsgewerbes berechtigt sind, sind auch zur Fahrzeug- und Transportbegleitung berechtigt.
...
(8) Die zur Ausübung des Gewerbes der Berufsdetektive sowie die zur Ausübung des Bewachungsgewerbes berechtigten Gewerbetreibenden dürfen zur Ausübung der ihren Gewerben vorbehaltenen Tätigkeiten (§ 129 Abs. 1 bzw. Abs. 4) nur Arbeitnehmer verwenden, die eigenberechtigt sind und die für diese Verwendung erforderliche Zuverlässigkeit und Eignung besitzen.
(9) Die im Abs. 8 genannten Gewerbetreibenden sind verpflichtet, der Bezirksverwaltungsbehörde, im Gebiet einer Gemeinde, für das die Landespolizeidirektion zugleich Sicherheitsbehörde erster Instanz ist, der Landespolizeidirektion, als Sicherheitsbehörde ein Verzeichnis aller Personen, die für eine der im § 129 Abs. 1 bzw. Abs. 4 genannten Tätigkeiten herangezogen werden, spätestens zwei Wochen vor dem Beginn ihrer Verwendung vorzulegen; jede Änderung hinsichtlich der für die im § 129 Abs. 1 bzw. Abs. 4 genannten Tätigkeiten herangezogenen Personen ist dieser Behörde binnen zwei Wochen anzuzeigen. Das Verzeichnis oder die Anzeigen von Änderungen dieses Verzeichnisses haben neben dem Vor- und Familiennamen der betreffenden Person auch deren Geburtsdatum, Geburtsort, Staatsangehörigkeit und Unterkunft (Wohnung) zu enthalten.
(10) Ist auf Grund bestimmter Tatsachen die Zuverlässigkeit einer gemäß Abs. 9 bekannt gegebenen Person nicht gegeben, so hat die Sicherheitsbehörde dem Gewerbetreibenden ohne unnötigen Aufschub schriftlich mitzuteilen, dass der Betroffene die erforderliche Zuverlässigkeit nicht besitzt.

Risiken:

Dateneinsicht durch Dritte

Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen

Beschreibung:

Zum Zwecke der Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen von Daten, werden Geheimhaltungsvereinbarungen mit deren externen Empfängern abgeschlossen.
Eine eigene Outsourcing-Leitlinie unterstützt die Entscheidungsträger um all unseren hohen Sicherheitsstandards gerecht zu werden. Die Outsourcing-Sicherheitsleitlinie gilt für alle Betriebsteile und ist bei der Konzeption von Outsourcing-Vorhaben zu beachten, wenn Dienstleistungen im Bereich Informationsverarbeitung betroffen sind, wie zum Beispiel bei den Projekten „I-Safety“ oder „I-Cos“. Bereits vor jeder Outsourcing-Entscheidung sind Sicherheitsaspekte zu bedenken und bei einer Ausschreibung zu berücksichtigen. Die Leitlinie ist gegenüber dem Outsourcing-Dienstleister als Prüfungsgrundlage zu nutzen und den Verträgen mit

Dienstleistern zugrunde zu legen.

Risiken:
Dateneinsicht durch Dritte

E-Mail-Verschlüsselung

Beschreibung:
Alle Exchange-Server wurden so konfiguriert, dass diese standardmäßig von allen Outlook-Clients eine Verschlüsselung einfordern wodurch die verschlüsselte, interne Unternehmenskommunikation via Mail sichergestellt wird.
Die geltende IT-Richtlinie §18 gibt vor, dass vertrauliche oder geheime Inhalte und Dokumente nicht via Mail an unternehmensexterne E-Mailkonten versandt werden dürfen. §17 regelt das Verbot automatisierter Weiterleitungen von Emails an externe Konten oder private mobile Geräte.

Risiken:
Dateneinsicht durch Dritte

Einrichtungen von Standleitungen bzw. VPN-Tunneln

Beschreibung:
Alle Filialen sind via LIC+ Leitungen angebunden und bilden das interne Firmennetzwerk. Den Zugriff auf das Firmennetzwerk von außen regelt eine redundant ausgelegte Firewall, welche auch ein VPN Gateway bereitstellt. Firmenlaptops ist es so möglich sich via VPN-Tunnel auch von außen sicher mit dem Firmennetzwerk zu verbinden.

Risiken:
Dateneinsicht durch Dritte

Kopieren von Dateien

Beschreibung:
Auszug aus der IT-Richtlinie:
§12 Das Kopieren von Dateien zum Zwecke der Heimarbeit oder zu privaten Zwecken ist strengstens untersagt!
§13 Das Abspeichern von Firmendaten auf externen Datenspeichern ist verboten! Darunter fallen auch Cloud Drives und ähnliche Technologien.

5. Eingabekontrolle

Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

Beschreibung:
Zur Erhöhung der Nachvollziehbarkeit erhält jeder neue User von IT-Systemen einen persönlichen IT-Account mit eigenem Passwort.

Risiken:
Verfälschung von Daten, Datenverlust

Protokollierung der Eingabe, Änderung und Löschung von Daten

Beschreibung:
Wesentliche im Einsatz befindliche Software verfügt über eine Protokollierung der Eingabe, Änderung und Löschung von Daten.

Risiken:
Verfälschung von Daten, unberechtigter Zugriff

Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Beschreibung:
Jeder User mit Zugang zu den IT-Systemen des Unternehmens erhält einen AD-Account welcher dem User genau die Zugangsrechte gewährt die für die Erfüllung seiner Aufgaben im Unternehmen benötigt werden. Darüber hinaus werden die Rechte zur Eingabe, Änderung und Löschung von Daten auch durch Software-Accounts geregelt.

Auszug aus der ÖWD Leitlinie zur Informationssicherheit:
"Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme ist eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen vergibt.
Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass Vertreter ihre Aufgaben erfüllen können."

Risiken:
Verfälschung von Daten, Datenverlust

6. Auftragskontrolle

Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

Beschreibung:

Es existiert eine Outsourcing Leitlinie welche Regelungen zur Sicherstellung der Informationssicherheit und des Datenschutzes im Falle des Outsourcings von IT-Leistungen vorgibt.

Auszug aus der Outsourcing Leitlinie des ÖWD:
4.1. Auswahl eines Outsourcing- Dienstleisters

Es ist selten erfolgversprechend, eine Geschäftsbeziehung lediglich auf Verträge und Regressansprüche zu begründen. Daher ist der Outsourcing-Dienstleister sorgfältig auszuwählen und eine vertrauensvolle und kooperative Zusammenarbeit anzustreben.
Bei der Auswahl ist zu prüfen, ob der Auftragnehmer als makellos, unbescholten und unbestechlich einzuschätzen ist (Zuverlässigkeit) und ob ein ernsthaftes und fachkundiges Betreiben der Dienstleistung gewährleistet ist (Seriosität).

Zu diesem Zweck sind folgende Punkte zu hinterfragen:
- Referenzen
- Kompetenz und Verfügbarkeit des Ansprechpartners
- Vertrauenswürdigkeit der Mitarbeiter
- Notfallplanung
- Zertifizierungen
- Dauer des Bestehens des Unternehmens
- finanzielle Situation des Unternehmens
- garantierte Verfügbarkeit (maximale Ausfallzeit)
- Sicherheitskonzept und Sicherheitsrichtlinien.

Für die Beurteilung sollte bei größeren Vorhaben eine Besichtigung des Outsourcing-Dienstleisters erfolgen.

Risiken:

Mißbräuchliche Verwendung der Personendaten

schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag)

Beschreibung:

Es existiert eine Outsourcing Leitlinie welche Regelungen zur Sicherstellung der Informationssicherheit und des Datenschutzes im Falle des Outsourcings von IT-Leistungen vorgibt.

Auszug aus der Outsourcing Leitlinie des ÖWD:
4.2. Vertragsspezifische Regelungen

Externen darf generell erst dann Zugang zu IT-Systemen und Anwendungen gewährt werden, wenn ein Vertrag unterschrieben wurde, der die Bedingungen für die Verbindung oder den Zugang definiert.
Im Vertrag ist schriftlich zu vereinbaren:
- Weisungsgebundenheit des Outsourcing-Dienstleisters
- Einhaltung der einschlägigen Gesetze, Vorschriften und internen Regelungen
- Stillschweigen über alle bekanntwerdenden Informationen
- technische und organisatorische Maßnahmen im Einflussbereich des Outsourcing-Dienstleisters und deren Kontrolle
- Melde- und Kommunikationswege
- Notfallvorsorgemaßnahmen
- Personaleinsatz durch den Outsourcing-Dienstleister
- Zutritts- und Zugangsrechte
- Regelungen für den Fall der nicht- oder mangelhaften Erfüllung
- Verfügbarkeitsanforderungen
- Rechte und Pflichten des externen Personals

- Regelungen zur Haftung
- Verfahren bei Beendigung des Vertrags (siehe Kapitel 4.5.5)

Risiken:
Mißbräuchliche Verwendung der Personendaten

Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

Beschreibung:
Es existiert eine Outsourcing Leitlinie welche Regelungen zur Sicherstellung der Informationssicherheit und des Datenschutzes im Falle des Outsourcings von IT-Leistungen vorgibt.

Auszug aus der Outsourcing Leitlinie des ÖWD:

4.5.5 Regelungen zum Ende der Tätigkeiten
Bei Beendigung des Auftragsverhältnisses muss eine geregelte Übergabe der Arbeitsergebnisse und der erhaltenen Unterlagen und Betriebsmittel erfolgen.
Es ist die ordnungsgemäße Funktion von gewarteten IT-Systemen zu überprüfen. Bei entsprechend gefährdeten IT-Systemen ist eine Virenüberprüfung durchzuführen.
Es sind außerdem sämtliche eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Außerdem sind ausscheidende Mitarbeiter explizit darauf hinzuweisen, dass die Verschwiegenheitsverpflichtung auch nach Beendigung der Tätigkeit bestehen bleibt.
Daten, die im Rahmen des Outsourcings extern gespeichert wurden, sind nach Abschluss des Auftrags vollständig und sicher zu löschen. Dies ist zu kontrollieren.

Risiken:
Mißbräuchliche Verwendung der Personendaten

Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis

Beschreibung:
Es existiert eine Outsourcing Leitlinie welche Regelungen zur Sicherstellung der Informationssicherheit und des Datenschutzes im Falle des Outsourcings von IT-Leistungen vorgibt.

Auszug aus der Outsourcing Leitlinie des ÖWD:
4.3. Organisation
...
Externe Mitarbeiter sind vor Beginn ihrer Tätigkeit einzuweisen und über hausinterne Regelungen und Vorschriften zur Informationssicherheit sowie die organisationsweite Leitlinie zur Informationssicherheit zu unterrichten.
Externe Mitarbeiter, die (eventuell) Zugang zu vertraulichen Unterlagen und Daten bekommen könnten, sind schriftlich auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen und zur Verschwiegenheit zu verpflichten.
...

Risiken:
Mißbräuchliche Verwendung der Personendaten

Vertragsstrafen bei Verstößen

Beschreibung:
In der mit allen externen Dienstleistern abzuschließenden NDA wird unter anderem auch das Strafmaß bei Vertragsverletzung geregelt.

Auszug aus der NDA:
§ 6 Ansprüche aus der Geheimhaltungsvereinbarung

6.1 Sofern ein Vertragspartner diese Geheimhaltungsvereinbarung nachweislich und schuldhaft verletzt, ist er zur Zahlung einer Konventionalstrafe in Höhe von EUR _____ für jeden Fall einer Vertragsverletzung an den jeweils anderen Vertragspartner verpflichtet.

6.2 Diese Pflicht zur Konventionalstrafe nach Punkt 6.1 besteht auch, wenn ein Dritter die Geheimhaltungsvereinbarung nachweislich und schuldhaft verletzt, sofern ihm die Informationen durch einen Vertragspartner zugänglich gemacht wurden.

6.3 Die Geltendmachung darüberhinausgehender Ansprüche bleibt den Vertragspartnern vorbehalten.

Risiken:

Mißbräuchliche Verwendung der Personendaten

vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen

Beschreibung:

Es existiert eine Outsourcing Leitlinie welche Regelungen zur Sicherstellung der Informationssicherheit und des Datenschutzes im Falle des Outsourcings von IT-Leistungen vorgibt.

Auszug aus der Outsourcing Leitlinie des ÖWD:
4.2. Vertragsspezifische Regelungen

Externen darf generell erst dann Zugang zu IT-Systemen und Anwendungen gewährt werden, wenn ein Vertrag unterschrieben wurde, der die Bedingungen für die Verbindung oder den Zugang definiert.
Im Vertrag ist schriftlich zu vereinbaren:

- Weisungsgebundenheit des Outsourcing-Dienstleisters
- Einhaltung der einschlägigen Gesetze, Vorschriften und internen Regelungen
- Stillschweigen über alle bekanntwerdenden Informationen
- technische und organisatorische Maßnahmen im Einflussbereich des Outsourcing-Dienstleisters und deren Kontrolle
- Melde- und Kommunikationswege
- Notfallvorsorgemaßnahmen
- Personaleinsatz durch den Outsourcing-Dienstleister
- Zutritts- und Zugangsrechte
- Regelungen für den Fall der nicht- oder mangelhaften Erfüllung
- Verfügbarkeitsanforderungen
- Rechte und Pflichten des externen Personals
- Regelungen zur Haftung
- Verfahren bei Beendigung des Vertrags (siehe Kapitel 4.5.5)

Risiken:

Mißbräuchliche Verwendung der Personendaten

7. Verfügbarkeitskontrolle

Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

Beschreibung:

Das Backupkonzept ist so ausgelegt, dass jegliche zentral in Salzburg gespeicherten Informationen an zwei unterschiedlichen Brandabschnitten gelagert werden. Die Daten auf den Filialservern werden täglich mit der Zentrale abgeglichen.
Der Exchange-Server, als eines der zentralen Kommunikationsmittel, verfügt über eine DAG (Database Availability Group) und ist somit speziell für hohe Verfügbarkeit und Ausfallsicherheit ausgelegt. Die DAG besteht aus zwei Postfachservern, von denen sich einer in Wien und einer in Salzburg befindet.
Lohn und Gehaltsdaten werden täglich auf Band gesichert. Die Bänder werden in einem feuerfesten Safe gelagert.

Risiken:

Datenverlust

Feuer- und Rauchmeldeanlagen

Beschreibung:

Die Gebäude verfügen über behördlich vorgeschriebene Brandmeldeanlagen nach ÖNORM F1000 (Feuerwehr und Brandschutzwesen).
Die technischen Richtlinien vorbeugender Brandschutz TRVB O 120, TRVB S114, TRVB N116, TRVB N 106 werden eingehalten.
Die ÖWD Brandschutzordnung liegt auf und regelt Zuständigkeiten, gibt Verhaltensregeln vor, während und nach einem Brandfall vor und enthält Evakuierungspläne,Sammelplätze und Fluchtwege.

Risiken:

Datenverlust

Feuerlöschgeräte in Serverräumen

Beschreibung:

In den Rechenzentren Salzburg und Wien sind Feuerlöscher vorhanden und deren Standorte ist gut sichtbar gekennzeichnet.

Risiken:

Datenverlust

Klimaanlage in Serverräumen

Beschreibung:

Die Serverräume sind redundant mit voneinander unabhängigen Klimaanlagen ausgestattet. Die Klimaanlagen werden jährlich gewartet.

Risiken:

Datenverlust

Schutzsteckdosenleisten in Serverräumen

Beschreibung:
Die im Einsatz befindlichen Verteiler entsprechen der Norm VDE 0185-305.

Risiken:
Datenverlust

Testen von Datenwiederherstellung

Beschreibung:
Die Rekonstruktion eines Datenbestandes wird in regelmäßigen Abständen geprüft.
Die Rekonstruktion von Daten mit Hilfe von Datensicherungsbeständen wird in jedem Fall nach jeder Änderung des Datensicherungsverfahrens getestet. Es wird sicherzustellt, dass eine vollständige Datenrekonstruktion möglich ist und geprüft ob die Verfahrensweise der Datensicherung praktikabel ist und die erforderliche Zeit zur Datenrekonstruktion den Anforderungen an die Verfügbarkeit entsprich.

Auszug aus der ÖWD Leitlinie zur Informationssicherheit: "
Datenverluste können nie vollkommen ausgeschlossen werden. Durch eine umfassende Datensicherung wird daher gewährleistet, dass der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen oder offensichtlich fehlerhaft sind. Informationen werden einheitlich gekennzeichnet und so aufbewahrt, dass sie schnell auffindbar sind."

Risiken:
Datenverlust

Unterbrechungsfreie Stromversorgung (USV)

Beschreibung:
Alle Serverräume sind mit einer ausreichend dimensionierten und jährlich gewarteten USV versorgt. Zusätzlich zu den USV Anlagen sind in den zwei Rechenzentren Salzburg und Wien Dieselaggregate im Einsatz um einen unterbrechungsfreien Betrieb der Server zu gewährleisten.
Alle Notstromgeneratoren sind mit einer unabhängigen Startvorrichtung ausgestattet, die automatisch aktiviert wird, wenn die Netzversorgung ausfällt.

Darüber hinaus verfügt das NSC über eine Notstromversorgung, basierend auf dem 1,5fachen des durchschnittlichen Bedarfs, über eine ausreichende Kapazität für den ununterbrochenen Betrieb von allen Kommunikations-, Meldungs-, Überwachungs-, Aufzeichnungs-, wichtigen Belüftungs- und Beleuchtungs-Einrichtungen einschließlich der Überwachungsanlagen für die Zeitdauer von mindestens 24 Stunden.
Ein Umschalten von oder zur Notstromversorgung beeinträchtigt den normalen Betrieb nicht.

Risiken:
Datenverlust

8. Trennungsgebot

Erstellung eines Berechtigungskonzepts

Beschreibung:
Auszug aus der ÖWD Leitlinie zur Informationssicherheit:
"Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme ist eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen vergibt.
Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass Vertreter ihre Aufgaben erfüllen können."

Risiken:
Datenverlust, Datenpanne

Festlegung von Datenbankrechten

Beschreibung:
Zugriff auf eine Datenbank ist "normalen" Usern ausschließlich über die vorgelagerten Softwareanwendungen inklusive deren Rechteverwaltung möglich. Lediglich Administratoren und führende Mitglieder des oberen Managements (Query-Tools) haben direkten Zugriff auf die Datenbanken.

Risiken:
Datenverlust, Datenpanne, unberechtigter Zugriff

Logische Mandantentrennung (softwareseitig)

Beschreibung:
Um zu verhindern, dass ein Anwender, von mehreren, voneinander unabhängigen Mandanten, versehentlich oder missbräuchlich auf die Daten eines anderen Mandanten zugreift, wird auf dem Datenbankserver auf logische Mandantentrennung zurückgegriffen.
Durch die Nutzung entsprechender mandantenspezifischer Accounts für den Datenzugriff und ein passendes Berechtigungskonzept kann dabei sichergestellt werden, dass jeweils nur mandanteneigene Daten gelesen oder verändert werden können. In diesem Szenario sind Zuordnungsfehler nur noch dann möglich, wenn der Fehler auch zu einer falschen Zuordnung des eingesetzten Datenbank-/Verzeichnisdienst-Accounts führt.

Risiken:
Datenverlust, Datenpanne

physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

Beschreibung:
Das Backupkonzept ist so ausgelegt, dass jegliche zentral in Salzburg gespeicherten Informationen an zwei unterschiedlichen Brandabschnitten gespeichert werden. Die Daten auf den Filialservern werden täglich mit der Zentrale abgeglichen.
Der Exchange-Server, als eines der zentralen Kommunikationsmittel, verfügt über eine DAG (Database Availability Group) und ist somit speziell für hohe Verfügbarkeit und Ausfallsicherheit ausgelegt. Die DAG besteht aus zwei Postfachservern, von denen sich einer in Wien und einer in Salzburg befindet.
Lohn und Gehaltsdaten werden täglich auf Band gesichert. Die Bänder werden in einem feuerfesten Safe gelagert.

Auszug aus der ÖWD Leitlinie zur Informationssicherheit: "
Datenverluste können nie vollkommen ausgeschlossen werden. Durch eine umfassende Datensicherung wird daher gewährleistet, dass der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen oder offensichtlich fehlerhaft sind. Informationen werden einheitlich gekennzeichnet und so aufbewahrt, dass sie schnell auffindbar sind."

Risiken:
Datenverlust, Datenpanne

Trennung von Produktiv- und Testsystem

Beschreibung:
Die Test und Schulungssysteme verwenden eigene Datenbanken und können somit die Produktivsysteme und deren Daten nicht beeinflussen.

Risiken:
Datenverlust, Datenpanne