Arbeitsanweisung: IT Sicherheit und Datenschutz

1. Zweck

- Sicherung der betrieblichen Daten gegen Verlust
- Sicherung der betrieblichen Daten gegen Zugang unbefugter Dritter

2. Beschreibung

2.1. Technische Ansprüche an die IT

Firewall

- Als Mindestanforderung muss im Betrieb eine Firewall zum Schutz vor Angriffen aus dem Internet vorhanden sein. Diese blockiert eingehenden und ausgehenden unerwünschten Datenverkehr (Aufruf unerwünschter Websites).

Virenschutz

- Jedes IT-Gerät ist durch einen eigenständigen Virenschutz zu schützen.
- Eine Firewall kann ebenso einen Großteil von Viren und Spam filtern, wenn diese Funktion freigeschalten wird.

W-LAN

- W-Lan Zugänge dürfen nie „offen“ (Zugang ohne Netzwerkschlüssel möglich) sein.
- Es wird empfohlen einen zusätzlichen Gastzugang einzurichten. Dieses muss so eingestellt werden, dass die Gäste keinen Zugriff auf Firmendaten bzw. das Firmennetz (z.B. zum Drucken) haben.

Zugänge zur betrieblichen IT

- Alle Zugriffsrechte und Auskunftsrechte obliegen ausschließlich der Geschäftsführung bzw. einer von dieser in der Stellenbeschreibung genannten Person
- Ein Passwort sollte mind. 8 Zeichen haben und Sonderzeichen enthalten.
- Für jeden Mitarbeiter mit Zugang zu einer PC-Arbeitsstation ist ein eigener Benutzername mit einem eigenen Passwort auf der Arbeitsstation selbst oder über eine Server-Verwaltung (ActiveDirectory/Verzeichnisdienst) einzurichten.
- Die Benutzernamen sollten Mitarbeitern eindeutig zuordenbar sein und nicht einer Funktion zugeordnet werden, um auch bei einem Personalwechsel eine Nachvollziehbarkeit der Zugriffe bzw. Bearbeitungen von Dateien sicher zu stellen.
- Eine gemeinsame Benutzung des gleichen Benutzernamens (z.B. "office") ist nicht zulässig.
- Die Passwörter für den Zugriff auf die technischen Geräte im Unternehmen sowie auf Online-Datenbanken sollten in regelmäßigen Abständen (z.B. einmal im Jahr) geändert werden.
- Alle Geräte sollten so eingestellt werden, dass sie nach spätestens 10 Minuten Inaktivität in den Ruhezustand wechseln. Zur weiteren Inbetriebnahme, muss das Passwort erneut eingegeben werden.
- Es wird empfohlen die Zugriffe auf die betriebliche IT mittels Musterformular Zugriffsliste zu regeln.

- Die Mitarbeiter müssen darauf sensibilisiert werden, den Computer beim Verlassen des Arbeitsplatzes herunter zu fahren und darauf zu achten, dass andere Personen keinen Einblick auf ihren Bildschirm haben, während sie personenbezogene Daten verarbeiten.

Server

- Der Aufstellungsort des Servers muss ohne direkte Sonneneinstrahlung in einem gekühlten und möglichst staubfreien Bereich sein.

- Einmal jährlich sollte der Server von einer Fachkraft geöffnet und gereinigt werden (sofern dadurch keine Garantieansprüche verletzt werden!).

- Server dürfen nicht als Arbeitsstation genutzt werden (z.B. zum Abrufen von Mails).

Hard Ware

- Der Anschluss von firmenfremder Hard Ware an jegliche Firmen IT ist untersagt. Ausgenommen sind Dienstleister mit einem Wartungsvertrag (siehe PB Gebäude- und Büroausstattung/IT).

Software

- Auswahlkriterien bei der Anschaffung bzw. Installation lt. PB Gebäude- und Büroausstattung/IT berücksichtigen

- Die genutzte Software ist im korrekten Ausmaß zu lizenzieren.

- Unlizenzierte Software (Raubkopien) sind untersagt bzw. zu entfernen.

Betriebssysteme

- Betriebssysteme sind, sofern keine andere Software dadurch beeinträchtigt wird, laufend zu aktualisieren.

- Die Aktivierung der „Bordmittel“ des Betriebssystems (z.B. Windows-Firewall, Windows-Defender, Mac-Firewall) ist sicher zu stellen.

- Optional: Bietet das Betriebssystem die Möglichkeit einer Datenverschlüsselung, so sind diese zu aktiveren.

Backup

- Es wird empfohlen durch einen IT-Dienstleister ein geeignetes Backup-Konzept erstellen zu lassen und umzusetzen. Dieses kann lokal oder online erfolgen.

- Bei einer rein lokalen Lösung gelten folgende Mindestvoraussetzungen:

    - Bei Vorhandensein eines Servers wird ein zentraler Netzwerkspeicher (NAS) mit mindestens zwei gespiegelten Festplatten empfohlen, zusätzlich müssen mindestens drei externen Festplatten für ausgelagerte Backups vorhanden sein, außer es ist eine externe Online-Sicherung (s.u.) vorhanden, dann ist eine externe Festplatte ausreichend. ACHTUNG: externe Backup-Platten sind laufend zu erstellen und auch vom Netzwerk oder der NAS zu trennen; die externen Speicher müssen an einem anderen Ort (z.B. zu Hause oder im versperrten und brandsicheren Dokumentenschrank aufbewahrt werden)

    - Bei Einzel – PCs: Personenbezogene Daten (Personalbuchhaltung und Rauchfangkehrerprogramm) sollten nur auf einem PC laufen, da dieser PC mit mindestens 3 externen Festplatten gesichert werden muss, außer es ist eine externe Online-Sicherung (s.u.) vorhanden, dann ist eine externe Festplatte ausreichend. ACHTUNG: externe Backup-Platten sind laufend zu erstellen und vom PC zu trennen; die externen Speicher müssen an einem anderen Ort (z.B. zu Hause oder im versperrten und brandsicheren Dokumentenschrank aufbewahrt werden)

- die lokale Sicherung muss mit Passwort gesichert werden

- Bei einer externen Online-Sicherung sollte auf folgende Punkte geachtet werden,
  - Der Online-Sicherungs-Anbieter sollte aus der EU stammen, die Daten sollten auch in der EU gespeichert werden und der Anbieter muss sich seinerseits zur Einhaltung der DSGVO und Datenschutz-Anpassungsgesetz 2018 verpflichten. Sollten Anbieter nicht aus der EU stammen, sollte die Liste der Firmen mit Vereinbarungen bezüglich Datenweitergabe in USA: https://www.privacyshield.gov/list konsultiert werden.

- Die Daten sollten beim online Backup verschlüsselt beim Anbieter gespeichert werden bzw. ist die Datenübertragung nur verschlüsselt (mindestens https) auszuführen.

- Ein Backup sollte so aufgebaut sein, dass mit der Zeit alte Backupdaten überschrieben werden, also gelöscht werden.

- Im Betrieb muss zusätzlich ein einfaches Backup vorhanden sein (s.o.)

Stromversorgung im Notfall

- Für den Fall einer Stromunterbrechung und zum Schutz der IT-Geräte sollte eine USV (unabhängige Stromversorgung) für die wichtigsten Geräte (Backup, Server, NAS) angeschafft werden um zumindest ein geregeltes Herunterfahren der Geräte zu ermöglichen

- Art und Umfang richten sich nach der Stromleistung der Geräte, die versorgt werden müssen und nach der Dauer, für die eine Stromversorgung sichergestellt werden soll.

- Eine Überbrückungszeit von mind. 15min wird empfohlen.

- Sollten Server oder NAS Geräte im Einsatz sein, so ist nach Möglichkeit darauf zu achten, dass die USV-Anlage diese Geräte bei Stromausfall "herunterfahren/ausschalten" kann, da andernfalls nach Ablauf der Überbrückungszeit für die Geräte die gleiche Situation eintritt wie bei einem Stromausfall.

- Achten Sie darauf, dass IT-Geräte durch einen Überspannungsschutz vor Stromspitzen geschützt sind.

2.2. Mobile Geräte

- Werden private Mobiltelefone (Handies) betrieblich genützt, dürfen diese nur zum Telefonieren und Fotografieren von Anlagen verwendet werden (Alle Fotos müssen sofort nach Versand in die betriebliche EDV gelöscht werden (s.u.) . Für private Mobiltelefone gelten aber ebenfalls alle folgenden Bestimmungen, soweit zutreffend. Daraus folgt, dass nur betriebseigene Geräte zur Nutzung als mobiles Kehrbuch verwendet werden dürfen.

- Um sicherzustellen, dass Daten von mobilen Geräten wie Notebooks, USB Sticks, Handys nicht an Dritte gelangen, müssen diese mit Passwörtern, SIM Pins usw. (siehe Zugänge) gegen unerwünschten Zugriff gesichert werden bzw. einzelne Ordner nach Möglichkeit verschlüsselt werden.

- Mobile Geräte dürfen nicht unbeaufsichtigt von Dritten genutzt werden, bzw. nur unter Aufsicht. Ausgenommen sind Dienstleister im Rahmen von Wartungstätigkeiten, wenn eine entsprechende Verschwiegenheitserklärung vorliegt (siehe PB Gebäude- und Büroausstattung/IT)).

- Mobile betriebliche Geräte dürfen nicht an firmenfremde Computer angeschlossen werden, betriebsfremde Geräte dürfen nicht an die betrieblichen Geräte angeschlossen werden

- Die Nutzung bzw. das Verschicken von betrieblichen Daten oder Kundendaten (z.B. Mängelfotos) von Whats App auf betrieblichen Mobiltelefonen ist untersagt (entspricht nicht der DSGVO), stattdessen kann z.B. die App von Signal oder imessage verwendet werden.

- Applikationen die nicht dem Firmenzweck dienen, sind generell zu vermeiden (Spiele udgl.).
- Geräte mit Firmendaten dürfen nie unbeaufsichtigt in öffentlich zugänglichen Bereichen sein.
- Mobile Geräte dürfen nicht in Fahrzeugen gelagert werden (Schutz vor Diebstahl und Wettereinflüssen).
- Verlust bzw. Diebstahl von Mobilen Geräten muss sofort der Geschäftsführung gemeldet werden. Für diesen Fall sollten die mobilen Geräte Fernlöschungsmöglichkeiten aufweisen.

2.3. Verarbeitung personenbezogener Daten

- Personenbezogene Daten in Papierform sollten aus Gründen der Datensicherheit als PDF auf einem, wie oben beschriebenen, gesicherten PC abgelegt werden.
- Das Abspeichern von personenbezogenen Daten auf externen Datenspeichern, wie z.B. Clouds, Dropbox udgl. ist untersagt.

2.4. Löschung personenbezogener Daten

- Werden personenbezogene Daten gelöscht (siehe auch PB Mitarbeiterausbildung und ArbeitnehmerInnenschutz und PB Erbringung der Dienstleistung), ist darauf zu achten, dass diese vollständig vom Speichermedium entfernt werden. Das Verschieben in den Papierkorb gilt nicht als löschen. Papierkörbe sollten in regelmäßigen Abständen geleert werden.
- Personenbezogene Daten dürfen erst nach Ablauf der Aufbewahrungsfrist lt. Liste Dokumente und Aufzeichnungen gelöscht werden.
- Bei der Löschung von elektronischen Daten ist darauf zu achten, dass die Daten von sämtlichen Systemen gelöscht werden (auch mobile Geräte, Backups usw.)
- Ist es erforderlich ein Backup wieder einzuspielen, so ist dafür zu sorgen, dass "gelöschte" Daten nicht wiederhergestellt werden.
- Werden personenbezogene Daten in Papierform im Betrieb vernichtet, ist darauf zu achten, dass ausschließlich Aktenvernichter verwendet werden, welche einen Partikel- oder Kreuzschnitt aufweisen.
- Werden personenbezogene Daten auf Papier von Abfallentsorgern entsorgt, muss ein Vernichtungszertifikat vom Entsorger ausgestellt werden.
- Bei der Entsorgung sämtlicher Altgeräte (auch mobile) ist darauf zu achten, dass diese auf die Standardeinstellung zurückgesetzt werden und sich keine personenbezogenen Daten mehr darauf befinden (**Vorsicht** Passwörter von Mitarbeitern abfragen, bevor sie die Geräte zurückgeben). Sollte dies nicht möglich sein, müssen Löschungs- bzw. Vernichtungszertifikate der Festplatten bzw. Geräte vom Entsorger eingefordert und aufbewahrt werden.

2.5. Private Daten von Mitarbeitern

- Es ist darauf zu achten, dass Mitarbeiter keine privaten Daten, wie z.B. Urlaubsfotos, auf Firmen IT. Geräten abspeichern.

2.6. Heimarbeit

- Zur sicheren Verbindung zum Firmen PC ist eine Firewall und eine VPN- Verbindung zu legen. Die VPN Verbindung stellt sicher, dass der Zugriff erst nach Eingabe eines separaten Passwortes möglich ist.

- Die Verbindung zum Firmen PC zum Zwecke der Heimarbeit darf nicht dauerhaft über Team Viewer oder ähnliches hergestellt werden.

- Das Kopieren von firmeninternen Daten für beispielsweise Heimarbeit ist untersagt

2.7. IT-Dienstleister

Für die Auswahl der IT Dienstleister und die Vertragsgestaltung siehe bitte PB Gebäude- und Büroausstattung/IT, Beschaffung

- Es wird empfohlen eine Dokumentation der IT erstellen zu lassen. Diese enthält mindestens:

  - welche Geräte mit welcher Konfiguration derzeit im Einsatz sind,

  - welche Maßnahmen zur Sicherung der Daten (Backup) ergriffen wurden,

  - welche Schutzmaßnahmen (Firewall, Virenschutz….) ergriffen wurden,

  - die Zuordnung der Benutzer, die Konfiguration des Servers, der Firewall, NAS etc.

  - und administrativen Kennwörter (zB Zugangsdaten zu Server, NAS, Firewall, Internetmodem)