IT SICHERHEIT - RICHTLINIEN

Dieses Dokument zur IT-Sicherheitsstrategie definiert die Sicherheitsanforderungen für die ordnungsgemäße und sichere Nutzung der IT-Dienste in Boyum IT. Ziel ist es, die Organisation sowie die Anwender so weit wie möglich vor Sicherheitsbedrohungen zu schützen, die ihre Integrität, ihre Privatsphäre, ihren Ruf und ihre Geschäftsergebnisse gefährden könnten.

Dieses Dokument gilt für alle Anwender in der Organisation, einschließlich temporärer Anwender, Besucher mit temporärem Zugang zu Dienstleistungen und Partner mit begrenzter oder unbegrenzter Zugriffsdauer auf Dienstleistungen.

1. IT VERMÖGENSWERTE - RICHTLINIEN

Der Abschnitt IT-Vermögenswerte-Richtlinien definiert die Anforderungen für den ordnungsgemäßen und sicheren Umgang mit allen IT-Posten in Boyum IT. Die Richtlinie gilt für Desktops, Laptops, Drucker und andere Geräte, für Anwendungen und Software, für alle Personen, die diese Ressourcen nutzen, einschließlich interner Benutzer, Zeitarbeiter und Besucher, und allgemein für alle Ressourcen und Fähigkeiten, die mit der Bereitstellung der IT-Dienstleistungen verbunden sind.

Verlust, Diebstahl, Beschädigung, Manipulation oder andere Vorfälle im Zusammenhang mit Vermögenswerten, die die Sicherheit gefährden, müssen dem IT Team so schnell wie möglich und unverzüglich gemeldet werden, vgl. Company Property Policy.

Bei der Arbeit von zu Hause aus (Home Office), liegt es in der Verantwortung eines jeden Mitarbeiters sicherzustellen, dass vertrauliche Informationen oder Boyum-IT-Ressourcen, auf die Zugriff besteht, für andere Personen unzugänglich sind. Anstatt Boyum IT Dateien auf dem persönlichen Computer zu speichern, sollten diese immer auf einem Boyum OneDrive oder einem Netzlaufwerk gespeichert werden, die von zu Hause aus leicht zugänglich sind. Dateien, die dorthin übernommen wurden, sollten anschließend sicher gelöscht werden. Für den Fall, dass ein Laptop oder mobiles Gerät gestohlen oder durch Malware oder einen Virus beschädigt wird, können die Daten sicher und einfach wiederhergestellt werden.

Die allgemeinen Regeln zur Erbringung von Arbeitsleistungen gelten unabhängig davon, ob die Arbeit zu Hause oder in den Büroräumen durchgeführt wird, z.B. die Regeln zur Vertraulichkeit und zum Umgang mit vertraulichen und sensiblen Informationen. Antiviren-Software muss auf allen privaten Computern, einschließlich Laptops, installiert und regelmäßig aktualisiert werden, wenn diese bei gelegentlicher Heimarbeit für die Ausübung der Arbeit mit Boyum genutzt werden. und regelmäßig aktualisiert werden. Lassen Sie nicht zu, dass Familienmitglieder Ihren Arbeitscomputer benutzen. - Verbindung unserer Arbeitsgeräte mit öffentlichen Hotspots vermeiden.

2. RICHTLINIE ZUR ZUGANGSKONTROLLE

Diese Richtlinie gilt für alle Benutzer in Boyum IT, einschließlich temporärer Benutzer, Besucher mit temporärem Zugang zu den Diensten, und Partner mit begrenzter oder unbegrenzter Zugangszeit zu den Diensten.

Es gibt eine Zugangsbeschränkung zu allen Büroeinrichtungen, entweder durch die Verwendung eines persönlichen Zugangscodes (das schließt Büros in Dänemark, Belgien, Ungarn und den USA ein, wo der Zugang zu den Gebäuden durch einen persönlichen Zugangscode kontrolliert wird) oder eines normalen Schlüssels (Büro in Spanien und Deutschland).

Aktivierung elektronischer Alarme außerhalb der regulären Bürozeiten.

Nur Personal in Schlüsselpositionen hat beschränkten Zugang zu den Infrastruktursystemen.

3. RICHTLINIE FÜR DEN FERNZUGRIFF / REMOTE

Es liegt in der Verantwortung der Angestellten / Freiberufler mit Zugriffsrechten auf das Firmennetzwerk von Boyum IT, sicherzustellen, dass deren Remote-Zugangsverbindung die gleiche Beachtung findet, wie die Vor-Ort-Verbindung des Benutzers zum Firmennetzwerk von Boyum IT.

SAP Business One
Der Zugriff auf unser eigenes SAP Business One ist außerhalb einer Boyum Niederlassung über Remote Desktop (RDP) möglich https://access.boyum-it.com. Melden Sie sich mit Ihren Anmeldedaten und Ihrem Domänenpasswort an. Über diesen Desktop kann auch auf den internen Dateiserver zugegriffen werden.

Sie müssen Mitglied einer Active Directory-Gruppe sein, um über RDP auf die Anmeldung zugreifen zu können. Das IT-Team kann Ihnen dabei behilflich sein.
Sie müssen Mitglied einer Active Directory-Gruppe sein, um sich über VPN anzumelden. Das IT-Team kann Ihnen dabei behilflich sein.

MariProject und interner File Server
Um auf MariProject und den internen Dateiserver zuzugreifen, können Sie den VPN-Client verwenden (derzeit verwenden wir Pritunl). Das IT-Team stellt eine VPN-Konfigurationsdatei zur Verfügung, damit eine VPN-Verbindung hergestellt werden kann. Auf allen Laptops, die vom IT-Team zur Verfügung gestellt werden, ist dies standardmäßig aktiviert.

Antivirus Software
Jeder Computer, der für die Arbeit mit Boyum IT verwendet wird, muss mit einer Antivirus-Software ausgestattet sein. Auch dann, wenn der eigene private Computer benutzt wird. Boyum IT stellt die Software zur Verfügung, aber

nur auf den Computern, die standardmäßig mit Boyum IT verbunden sind. Das IT Team kann kontrollieren, welche Computer mit Boyum IT Servern verbunden sind. Laptops, die vom IT-Team zur Verfügung gestellt werden, sind standardmäßig mit Antivirus-Software ausgestattet und DÜRFEN NICHT deinstalliert werden.

Bei der Nutzung des privaten Computers zur Verbindung mit Boyum IT via VPN, ist es erforderlich, diesen Computer mit einem Bildschirmschoner mit aktiviertem Passwort zu sichern, um zu verhindern, dass sich jemand an Ihrem Computer zu schaffen macht oder auf das Boyum IT-Netzwerk zugreift.

Zum Schutz unserer Daten, unseres Systems, unserer Benutzer und Kunden befolgen und nutzen wir diese Vorsichtsmaßnahmen:

- Zentralisierung der Installation, Verwaltung und Aktualisierung von Antiviren-Software auf allen Systemen unter Verwendung eines cloud-basierten Antiviren-Systems mit BitDefender
- Regelmäßige Aktualisierung der Systemsoftware (OS) - die von Windows Server Update Services (WSUS) gesteuert wird
- Einsatz von administrierten Firewalls PFsense an allen unseren Standorten
- Verwendung der automatischen Bildschirmsperre bei allen unseren IT-Systemen nach 10 Minuten Inaktivität. Passwort muss eingegeben werden, um das System wieder zu öffnen
- Bereitstellung des Remote-Zugriffs über verschlüsselte Microsoft RDC, & VPN
- Implementierung der Netzwerktrennung mittels IPSEC Site-to-Site-VPN und VLAN-Trennung zu allen Außenstellen.
    - Wartung von Backups an separaten Standorten (Remote-Backup-Standort für wichtige Daten)
    - Implementierung einer redundanten Lösung über virtuelle Serverumgebungen (VMware-Cluster mit Failover).
- Speicherung der Daten in einem Rechenzentrum, das über eine Zugriffskontrolle mit Zugriffsprotokollierung, Kühleinrichtung, Redundanzstromversorgung einschließlich USV verfügt.

4. RICHTLINIE ZUR PASSWORT-KONTROLLE

Das IT-Team teilt zu Beginn ein temporäres Passwort zu. Dieses können Sie beim ersten Einloggen ändern. Voraussetzung dafür ist eine ordnungsgemäße Passwortkontrolle. Dies gilt sowohl im Büro als auch von unterwegs. Vermeiden Sie Passwörter wie ‘guest’, ‘password’, ‘123456’ oder ‘qwerty’.

Ein gutes, Boyum IT sicheres Passwort erfüllt die folgenden Kriterien:

- keines der zuletzt verwendeten 24 Passwörter darf erneut verwendet werden
- Das maximale Alter von Passwörtern beträgt 185 Tage
- Das Mindestalter für Passwörter beträgt 1 Tag
- Die Mindestlänge des Passwortes beträgt 12 Zeichen
- Sollte nicht den Kontonamen des Benutzers und auch keine Teile des vollständigen Namens des Benutzers, mit mehr als zwei aufeinanderfolgenden Zeichen enthalten
- Sollte Zeichen aus mindestens drei der folgenden vier Kategorien enthalten:
    - Englische Großbuchstaben (A bis Z)
    - Englische Kleinbuchstaben (a bis z)
    - Einfache Ziffern (von 0 bis 9)
    - Nichtalphabetische Zeichen (z.Bsp., !, $, #, %)
- Kontosperre = bei 5 ungültigen Anmeldeversuchen

Das Merken all dieser Zahlen und Symbole kann schwierig sein, daher versuchen Sie es mit einer Eselsbrücke. Auch die Zwei-Faktor-Authentifizierung ist ein nützliches Hilfsmittel. Das bedeutet, dass Sie sowohl ein Passwort als auch eine verlinkte E-Mail oder Kontaktinformationen benötigen, um zu bestätigen, dass Sie wirklich auf Ihr Arbeitsmaterial zugreifen.

5. DER DATENVERARBEITER

- Der Datenverarbeiter wird regelmäßig an Fortbildungen zur Wachsamkeit in Bezug auf IT-Sicherheit und Verarbeitung personenbezogener Daten durchführen. Der Datenverarbeiter wird auch die Aufgabentrennung in Bezug auf die Zugangskontrolle und die Rechteverwaltung umsetzen, weitere Sicherheitsmaßnahmen sind in Planung.

- Der Datenverarbeiter wird die technische Sicherheit fortlaufend evaluieren und Upgrades vornehmen, wenn diese neuen Technologien die Systeme sicherer machen können, und zwar zu Kosten, die der Datenverarbeiter im Vergleich zum Sicherheitsbedarf für angemessen hält.

Alle Fragen zu internen Systemen, Software oder Hardware können direkt an it@boyum-it.com gerichtet werden.