Unternehmenskommunikation/Richtlinien für Mitarbeiter

-generell sollten alle Daten geschützt werden (Excel, Laptop, Festplatte)

1. Hardware

Firmenhandy/Firmentablet

-ob man Handy mit Heim nehmen muss/darf, ist von Firma geregelt

-nicht für private Zwecke

-keine öffentlichen Netzwerke, nur mit VPN

-nur Apps installieren, die von Firma freigegeben sind (evtl auch eigener App Store)

-kein externer darf auf Diensthandy zugreifen (sensible Daten)

-Passwortgeschützt

PC

-Software kann/darf nicht installiert werden (z.B. Chrome, manche Installationen können nur von Admin installiert werden)

-private Nutzung wird vom Arbeitgeber festgelegt

-VPN Verbindung bei Homeoffice/öffentlichen Netzwerken

-Passwort Sicherheit (regelmäßige Änderung, Keypass)

-Firewall/Anti Virus

USB/Festplatten

-keine externen USBs

-verschlüsselte USBs sollten genutzt werden

-Vermeidung von USBs, Festplatten könnte eine Lösung sein

Bring your own Device

-Zertifikate runterladen

-WLAN/VPN

-evtl darf eigens Handy nicht mitgebracht werden

2. Software

E-Mail

-Server sollte verschlüsselt sein

-Passwörter nur per Mail, da verschlüsselt

-CI, Firmendesign, Signatur

-formale Kriterien

-Einheitlichkeit

-Überprüfung der Anhänge

-nicht für private Angelegenheiten nutzen

Social Media

-Firma wird repräsentiert: Likes, Kommentare im Rahmen der Firma (z.B. keine Beleidigungen)

-auf Postings achten, die im negativen Sinne mit Firma in Verbindung gebracht werden: nicht liken, etc

-„positives“ Verhalten auf social Media wirft auch positives Licht auf Firma

-Kommunikation angepasst an die Unternehmenswerte

- Unternehmen soll hashtag vorgeben

Inhalte kommunizieren:

- Guidelines via Intranet verbreiten
- Visuell schön gestalten: Anschauliche Gestaltung, Handlungshinweise wie soll mans machen, wie nicht?! Symbole, Zeichen, Animationen, Schulungsvideo
- Competition auf Social Media: „Wer postet das beste Foto im Büro?“