Bitte beachten sie beim bearbeiten von Emails folgende Punkte:

1. **Bitte überprüfen Sie Ihre Emails sorgfältig!**

2. **Keine Anhänge von unbekannten Absendern öffnen.**

   Aber selbst bei bekannten Absendern ist immer Vorsicht geboten, wenn Anhänge mitgeschickt wurden. Besonders gegenüber folgenden Datentypen in Anhängen sollte man misstrauisch sein:
   .asf, .pdf. exe, .avi, .mov, .mpg, .bat, .scr, .zip, .rtf, .doc, .pif, .reg sowie .vbs.

   Im Zweifel melden Sie sich bei uns, damit wir diese Email per Fernwartung überprüfen können, oder fragen Sie - wenn der Absender bekannt ist – doch bei diesem nach, ob das mit dem Anhang seine Richtigkeit hat.

3. Emails sollten **!NIEMALS!** mit einem auf dem Server installierten Emailprogramm abgeholt werden. Wenn Sie sich nicht sicher sind, ob das bei Ihnen der Fall ist, bitten wir um kurze Rückmeldung, damit wir das überprüfen und gegebenenfalls ändern können.

4. **Ein Virenscanner ist Pflicht!**

5. Damit der **Virenscanner immer aktuell** ist, sollten sich die Mitarbeiter rechtzeitig vor Ablauf der Virenscanner-Laufzeit melden.

6. **Unsichere Webseiten vermeiden.**
   Links in Phishing-Mails führen nicht selten zu betrügerischen Webseiten, die von dem sicheren Original optisch nicht zu unterscheiden sind. Vor dem Klick auf etwaige Buttons oder Links sollte einmal die Web-Adresse überprüft werden, die in der linken unteren Ecke des Browsers oder Mailclients angezeigt wird, wenn man den Mauszeiger über den Link fährt. Ist hier eine URL abzulesen, die nichts mit dem Namen der besuchten Webseite oder des Webseiten-Betreibers zu tun hat, sollte man auf den Klick verzichten.

7. **Privates Surfen am Arbeitsplatz sollte auf das notwendigste beschränkt werden** oder von einem Rechner ausgeführt werden, der keine Verbindung zu sensiblen Daten hat.