Security Policy
Richtlinie für die IT-Sicherheit der Arbeitsplätze[1]

Diese Richtlinie für die IT-Sicherheit gilt für .....
(Unternehmen/Organisation)
Für alle Fragen der IT-Sicherheit ist ..... der zuständige Ansprechpartner.

A. Unsere IT ist wie folgt geschützt:

Virenschutz	☐ am Arbeitsplatz		☐ am Gateway ins Internet
Hackerschutz (Firewall)	☐ am Arbeitsplatz		☐ am Gateway ins Internet
Spamfilter	☐ am Arbeitsplatz		☐ am Gateway ins Internet
Web-Authentifizierung/-Filterung	☐ vorhanden		☐ nicht vorhanden
Mitarbeiter-Zugriff von außen	☐ gesichert	☐ nicht gesichert	☐ nicht erlaubt
Zentrales Backup	☐ vorhanden		☐ nicht vorhanden
Sonstiger Schutz			

B. Die folgenden Regeln sind von allen Mitarbeitern zu beachten, um Schäden abzuwehren und die Arbeitseffizienz zu sichern.

1. Die eingerichteten **Schutzmechanismen** dürfen **nicht unerlaubt unterlaufen** werden (z.B. sind das Ausschalten des Virenscanners oder zusätzliche, ungeschützte Verbindungen ins Internet verboten).
2. Jeder **Zugriff auf Unternehmensdaten** muss betrieblich veranlasst sein, die Weitergabe an Dritte ist nur nach vorheriger Ermächtigung gestattet.
3. **Lizenzbestimmungen** sind einzuhalten. Private Software ist auf betrieblichen Systemen (nicht) erlaubt.
4. Die **private Nutzung** des Internets ist (in Maßen) (nicht) erlaubt (, jedoch nur in den Pausenzeiten und nach separater Richtlinie "Privatnutzung des Internets").
5. Betriebliche Daten gehören ins zentrale **Backup**, andernfalls muss mindestens einmal (zweimal) pro Woche eine Sicherungskopie hergestellt werden. Die Lesbarkeit der Sicherungskopie ist zu prüfen.
6. **Email-Anhänge** von unbekannten Absendern sind sofort zu löschen.
7. Externe Speichermedien (z.B. **USB-Sticks**) sind mit einem Virenscanner zu prüfen. Die Aktualität der Virendatenbank muss mindestens einmal pro Tag automatisch überprüft werden.
8. **Vertrauliche Daten** müssen verschlüsselt werden. Beim Löschen von vertraulichen Daten muss ein sicheres Verfahren angewendet werden.
9. IT-Arbeitsplätze sind bei Verlassen zu sperren; es ist eine **Bildschirmsperre** mit Passwortschutz einzusetzen, die sich spätestens nach 5 Minuten Inaktivität automatisch einschaltet.
10. Es müssen gute **Passwörter** eingesetzt werden und alle Passwörter sind geheim zu halten.
11. .....
12. .....

Zur Kenntnis genommen:

....
Ort, Datum, Unterschrift Geschäftsleitung Ort, Datum, Unterschrift Mitarbeiter/in

[1] Diese Richtlinie gilt für die IT-Arbeitsplätze. Für zentrale Server und den IT-Betrieb sind weitere Regeln nötig (z.B. Zyklus Virenpatternupdate am Gateway, Firewall, Patch Management, Zugangsschutz, Backup und Restore, Rechtevergabe uam.)