SJT SOLUTIONS
IT - MANAGED SERVICES - CONSULTING

Cyberversicherung

Die 50 wichtigsten Pflichten (Obliegenheiten) – Checkliste

für Geschäftsführer & Entscheider

NR.	Was muss umgesetzt sein?	Warum ist das wichtig?	Vorhanden	Nicht vorhanden
1	**Mindestens täglich** wird ein Backup aller wichtigen Daten gemacht.	Damit im Ernstfall nichts verloren geht.	☐	☐
2	Es gibt **mehrere Sicherheitskopien**, davon eine **außerhalb des Firmennetzes.**	Schutz bei Feuer, Diebstahl oder Verschlüsselung.	☐	☐
3	Es wurde **mindestens einmal getestet**, ob das Backup wirklich wiederherstellbar ist.	Damit Sie im Notfall nicht ohne Daten dastehen.	☐	☐
4	Es wird ein **zweiter Faktor beim Login** (z. B. Handycode) verwendet	Verhindert Datenklau bei Passwortdiebstahl.	☐	☐
5	Es werden **keine alten oder abgelaufenen Windows-Versionen** verwendet.	Alte Systeme haben Sicherheitslücken.	☐	☐
6	**Updates und Sicherheitslücken** werden regelmäßig geschlossen.	Angriffe nutzen bekannte Lücken.	☐	☐
7	Es gibt eine richtige **Business-Firewall** mit Überwachung.	Eine Fritzbox reicht nicht.	☐	☐
8	Das Netzwerk ist **in Bereiche aufgeteilt** (z. B. Büro, Server).	Schützt, wenn ein Gerät infiziert wird.	☐	☐
9	Auf jedem Gerät ist ein **aktueller Virenschutz** installiert.	Basis-Schutz vor Schadsoftware.	☐	☐
10	**Passwörter** werden sicher aufbewahrt – z. B. mit einem Passwort-Programm.	Kein Zettel im Schreibtisch.	☐	☐

NR.	Was muss umgesetzt sein?	Warum ist das wichtig?	Vorhanden	Nicht vorhanden
11	**Admins arbeiten nicht im Alltag** mit vollen Rechten.	Minimiert Schaden bei Fehlern oder Angriff.	☐	☐
12	Techniker oder IT-Firmen haben eigene **Zugänge mit Protokollierung.**	Transparenz & Nachvollziehbarkeit.	☐	☐
13	Fernzugriff auf das Büro erfolgt nur **verschlüsselt und mit Sicherheitscode.**	Schutz vor unbefugtem Zugriff.	☐	☐
14	**Aktivitäten werden überwacht**, z. B. wer sich wann anmeldet.	Frühzeitige Warnung vor Angriffen.	☐	☐
15	Es gibt eine **Alarmanlage für die IT** (Monitoring).	Reagieren bevor der Schaden groß ist.	☐	☐
16	Alle Mitarbeitenden erhalten **regelmäßige Schulungen zur IT-Sicherheit.**	Phishing-Mails sind oft der Anfang.	☐	☐
17	Es werden **Phishing-Tests** gemacht, um Mitarbeiter zu sensibilisieren.	Praxis ist der beste Lehrer.	☐	☐
18	Auch **Geschäftsführung wird geschult.**	Chefs sind oft das Ziel von Angriffen.	☐	☐
19	Es gibt einen **Notfallplan**, wer was im Ernstfall macht.	Klare Rollen sparen Zeit.	☐	☐
20	Der Notfallplan wurde schon **einmal geübt.**	Theorie ist gut – Praxis ist besser.	☐	☐
21	Ehemalige Mitarbeiter haben **sofort keinen Zugriff mehr.**	Zugang muss entzogen werden.	☐	☐
22	Es gibt eine **Liste aller Geräte** im Unternehmen.	Was man nicht kennt, kann man nicht schützen.	☐	☐
23	Handys und Laptops sind **gesichert und fernlöschbar.**	Schutz bei Verlust oder Diebstahl.	☐	☐
24	E-Mails werden durch **Filter & Sicherheitsregeln** geprüft.	Weniger Spam & gefährliche Mails.	☐	☐
25	**USB-Sticks sind gesperrt** oder werden überwacht.	Schutz vor Schadsoftware.	☐	☐

NR.	Was muss umgesetzt sein?	Warum ist das wichtig?	Vorhanden	Nicht vorhanden
26	Laptops sind **verschlüsselt.**	Verlorene Geräte = keine Datenlecks	☐	☐
27	Tests und Experimente finden **nicht im Live-System statt.**	Vermeidung von Ausfällen.	☐	☐
28	Mitarbeitende im Homeoffice nutzen **sichere Geräte und Zugänge.**	Firmen-Daten gehören nicht auf Privatgeräte.	☐	☐
29	Die IT-Firma oder Dienstleister wurden **geprüft.**	Vertrauen ist gut – Kontrolle besser.	☐	☐
30	Neue Programme dürfen **nur nach Freigabe** installiert werden.	Schutz vor gefährlicher Software.	☐	☐
31	Alte Geräte werden **sicher entsorgt oder gelöscht.**	Keine Datenreste für Dritte.	☐	☐
32	Nur **sichere Verbindungen und Protokolle** werden genutzt.	Alte Technik = Sicherheitslücken	☐	☐
33	Freigaben auf Servern sind nur **für berechtigte Personen.**	Nicht jeder braucht alles.	☐	☐
34	Es gibt eine **Strom-Absicherung** für Server	Stromausfall = Datenverlust	☐	☐
35	Der Internetzugang ist **gefiltert** (z. B. keine gefährlichen Seiten)	Schützt vor versehentlichem Zugriff.	☐	☐
36	Sicherheitswarnungen werden **auch gelesen & bearbeitet.**	Nicht ignorieren – handeln.	☐	☐
37	Externe Zugriffe sind auf **bestimmte Zeiten oder Orte beschränkt.**	Weniger Risiko durch Kontrolle.	☐	☐
38	Änderungen in der IT werden **dokumentiert.**	Fehler können schneller behoben werden.	☐	☐
39	Das Unternehmen erfüllt die **DSGVO-Vorgaben.**	Datenschutz ist Pflicht.	☐	☐
40	Wichtige E-Mails sind **verschlüsselt**	Niemand liest ungewollt mit.	☐	☐

NR.	Was muss umgesetzt sein?	Warum ist das wichtig?	Vorhanden	Nicht vorhanden
41	Alte Daten werden regelmäßig **gelöscht.**	Schutz vor Abfluss & Aufräumen.	☐	☐
42	Es gab einen **externen Sicherheitstest** (z. B. IT-Check)	Blick von außen deckt Lücken auf.	☐	☐
43	Admin-Zugänge sind **nicht direkt vom Internet aus erreichbar.**	Kein offenes Tor für Angreifer.	☐	☐
44	Es gibt einen **Plan für den Weiterbetrieb im Notfall.**	Geschäft geht weiter trotz IT-Ausfall.	☐	☐
45	Die **Versicherungsbedingungen** wurden gelesen & dokumentiert.	Keine bösen Überraschungen.	☐	☐
46	Es gibt **eine IT-Sicherheitsbeauftragte Person.**	Jemand hat das Thema im Blick.	☐	☐
47	M365 und Cloud-Dienste werden regelmäßig **geprüft & bereinigt.**	Externe dürfen nicht mehr sehen als nötig.	☐	☐
48	Router & Firewalls werden **regelmäßig aktualisiert.**	Schutz vor neuen Angriffen.	☐	☐
49	Es gibt klare Regeln für **Reaktion auf IT-Warnungen.**	Damit niemand wegschaut.	☐	☐
50	Die Firma ist gegen **soziale Täuschung (Social Engineering)** sensibilisiert.	Technik reicht nicht – Menschen müssen mitmachen.	☐	☐

Deine digitalen Bodyguards!