IT-Quick-Check

Sind Sie mit Ihrem Unternehmen zum Thema IT gut aufgestellt?

Mit dieser Checkliste können Sie sich schnell einen Überblick verschaffen – und wenn Sie Bedarf identifizieren, die entsprechenden Maßnahmen ableiten. Wir unterstützen Sie gern – bei der Analyse Ihres Quick-Checks, bei der Priorisierung der ToDo's und bei der Umsetzung der notwendigen IT-Projekte.

Sicherheits-Management und IT-Technik	**Ja**	**Nein**
Gibt es einen IT-Sicherheitsbeauftragten?	❑	❑
Gibt es eine Liste, in der die Zuständigkeiten und Verantwortlichkeiten für die Umsetzung der systemkritischen und allgemeinen IT-Sicherheitsmaßnahmen festgelegt sind?	❑	❑
Werden Virenschutzprogramme flächendeckend eingesetzt und ständig aktualisiert?	❑	❑
Sind Firewall-Lösungen vorhanden und werden diese eingesetzt?	❑	❑
Gibt es Regelungen zu Dateiübertragungen und Nachrichtenaustausch mit externen Kontakten? (schließt auch die Herausgabe / Weitergabe / Nutzung von Datenträgern wie USB-Sticks ein)	❑	❑
Gibt es ein Rollen- und Rechtekonzept für die Zugriffe auf unterschiedliche IT-Systeme?	❑	❑
Gibt es dokumentierte Prozesse zum Mitarbeiter-Eintritt und -Austritt in das/ aus dem Unternehmen, in denen auch die IT-Zugriffsrechte geregelt sind?	❑	❑
Haben Sie einen Datenschutz-Verantwortlichen bzw. -beauftragten benannt?	❑	❑
Allgemeine Sicherheitsaspekte, Sicherheitsbewusstsein und Verhalten in Notfällen	**Ja**	**Nein**
Wissen alle Benutzer, wie sie sicherheitskonform handeln und Risiken beim Internetzugriff sowie beim Empfangen und Versenden von Emails vermeiden?	❑	❑
Sind die Mitarbeiter ausreichend für die Internetnutzung und den Email-Einsatz geschult?	❑	❑
Wissen alle Benutzer, wie sie sich verhalten sollten, wenn ein Virenschutzprogramm einen Schadprogramm-Befall meldet?	❑	❑
Werden ausführliche Installations- und Systemdokumentationen insbesondere zu systemkritischen IT-Lösungen erstellt und regelmäßig aktualisiert?	❑	❑
Gibt es einen Notfallplan für alle wichtigen Notfallsituationen, der außer detaillierten Verhaltensanweisungen auch (aktuelle!) Namen und Kontaktdaten von verantwortlichen Ansprechpartnern enthält (inklusive Ansprechpartner außerhalb der regulären Arbeitszeit)?	❑	❑
Kennwörter, private Nutzung von IT-Zugängen	**Ja**	**Nein**
Sind alle Mitarbeiter in der Vergabe sicherer Kennwörter geschult und werden diese regelmäßig geändert?	❑	❑
Gibt es eine Regelung für privates Surfen und private Email-Korrespondenz?	❑	❑
Datensicherung	**Ja**	**Nein**
Gibt es eine Datensicherung, getrennt vom PC / Server?	❑	❑
Werden die Sicherungssätze an unterschiedlichen Orten innerhalb und außerhalb des Unternehmens verteilt aufbewahrt?	❑	❑
Ist berücksichtigt, dass die Daten in mehreren Sicherungssätzen gesichert und ältere Sicherungen (Historien) mit neueren Sicherungen überschrieben werden?	❑	❑
Sind die Sicherungs- und Rücksicherungsverfahren dokumentiert? Wird dies regelmäßig getestet?	❑	❑

ATD GmbH
Linnéstraße 5 | 38106 Braunschweig
Telefon 0531 238 24 0 | Fax 0531 233 55 61
bewerbung@atd.de | www.atd-systemhaus.de

Drahtlose Netzwerkverbindungen (WLAN) und Hotspots	Ja	Nein
Wurden bei WLAN-Access-Points und WLAN-Routern die werkseitig eingestellten Kennwörter geändert? Werden die Kennworte für Gast-Zugänge regelmäßig geändert?	❑	❑
Ist auf den WLAN-Komponenten die WPA2-Verschlüsselung aktiviert?	❑	❑
Software-Nutzung und Software-Updates	**Ja**	**Nein**
Werden Sicherheits-Updates regelmäßig eingespielt? (Das umfasst nicht nur Clients und Server sondern auch andere Netzwerkkomponenten wie Firewalls, Router, Switchte, AccessPoints etc. für die es Software- oder Firmware-Updates gibt, die Sicherheitslücken schließen.)	❑	❑
Schutzvorkehrungen und Schutzeinrichtungen	**Ja**	**Nein**
Sind die Server des Computersystems ausreichend gegen Feuer, Überhitzung und Wasserschäden geschützt?	❑	❑
Gibt es eine Zutrittskontrolle? (zum Gebäude / zum Raum mit der Serveranlage)	❑	❑
Ist der Bestand von Hard- und Software in einer Inventarliste erfasst und werden regelmäßige Bestandskontrollen durchgeführt?	❑	❑
Gibt es ein Lizenzmanagement?	❑	❑
Gibt es Wartungsverträge für die Hardware und ggfs. für die genutzte Software?	❑	❑
Mobile Endgeräte	**Ja**	**Nein**
Gibt es ein Sicherheitskonzept für den Einsatz mobiler Endgeräte inklusive geregelter Verantwortlichkeiten für das Management derselben mit geeigneten Lösungen?	❑	❑
Sind die notwendigen Prozesse bei Diebstahl/ Verlust von mobilen Geräten bekannt?	❑	❑

Quick-Check Feedback

Ihre nächsten Schritte

- Überprüfen Sie ihre Antworten selbstkritisch: Können Sie mit einem klaren „Ja" antworten – oder vermuten und hoffen Sie, dass dieser Punkt gut geregelt ist?
- Bei allen Antworten, bei denen Sie nicht ganz sicher sind: Fragen Sie ihre IT-Mitarbeiter und Experten, wie es tatsächlich geregelt ist.
- Wenn Sie den Quick-Check beantwortet haben – fragen Sie stellvertretend einige Mitarbeiter zu den jeweils relevanten Themen – sind die Prozesse/ Regelungen tatsächlich bekannt?
- Sie haben Lücken entdeckt / aufgedeckt? Wir unterstützen Sie gern in der Risiko-Analyse und in der Priorisierung der durchzuführenden Maßnahmen.

Sie wünschen weitere Unterstützung? Senden Sie uns dieses Blatt einfach ausgefüllt per Email an vertrieb@atd.de oder als Fax an 0531 2335561 und die passenden Experten werden sich umgehend bei Ihnen melden.

Firma: _____ Ort: _____

Name: _____ Position: _____

· Bitte rufen Sie mich unter dieser Telefon-Nummer an: _____

· Bitte vereinbaren Sie einen Termin mit mir in ca. · 1 Woche · 2 Wochen · 4 Wochen

Wir unterstützen Sie gern bei einer Detail-Analyse Ihrer IT-Risiken!