Toolbox KMU.DIGITAL 2.0
IT-Security – bilingual checklist

Developed by WKÖ – Austrian Federal Economic Chamber
Translation: EUROCHAMBRES Digital Services Network

1	Regelung des Zuganges zu betrieblicher Hardware	Rules on access to company operational hardware
1-1	Sind Räume mit betrieblicher EDV-Ausstattung gesichert?	Are the rooms with operational IT equipment physically secured?
1-2	Verfügen Sie über Überwachungseinrichtungen (Zutrittssysteme, Videoüberwachung, etc.)?	Do you have monitoring facilities (access systems, video surveillance etc?)
1-3	Wurden Zugangsberechtigungen festgelegt?	Did you determine access rules?
1-4	Gibt es Sicherheitsvorkehrungen bei Reinigungs- und Wartungsarbeiten?	Are there any safety rules for cleaning and maintenance activities
1-5	Gibt es Sicherheitsvorkehrungen bei Telearbeit (Netzwerkzugang von außen)?	Are there any safety rules for telework (use of hardware and remote access to the network?

2	Regelung des Zugriffes auf Daten	Rules on Data Access
2-1	Gibt es ein Benutzeridentifikations- und ein Passwortverfahren für technische Geräte?	Did you determine user identification and password procedures for IT devices?
2-2	Verfügen Sie über Systeme zur Protokollierung von Zugriffen auf Daten und deren Kontrolle?	Do you have systems for logging access records and control?
2-3	Verfügen Sie über eine Dokumentation der Eingabeverfahren?	Do you record who provides which input to the database?
2-4	Sind automatische Bildschirmsperren (Passwortschutz bei Arbeitspausen) aktiviert?	Are workstations automatically locked (during pauses and is the password required to unlock)?
2-5	Sind automatische Zugangssperren bei wiederholten Anmelde-Fehlversuchen aktiviert?	Are workstations automatically blocked in the event of repeated login attempts?
2-6	Gibt es individuelle Benutzerkonten für Mitarbeiter/innen?	Are there individual accounts for each employee?
2-7	Werden Datenträger verschlüsselt, insbesonders jene mit personenbezogenen Daten?	Are data carriers and storage media, in particular those with personal data, encrypted?
2-8	Gibt es ein Berechtigungskonzept und ein Verfahren für die Vergabe von Zugriffsrechten auf Basis des Betriebssystems?	Do you have a concept in place that regulates authorisation and access rights based on the operating system?

2-9		Verfügen Sie über einen Schutz vor unberechtigten Zugriffen auf IT-Systeme (Firewall, etc.)?	Is there a protection system against unauthorised access to IT systems in place (firewalls etc)?
2-10		Werden mobile Datenträger verwaltet, damit bekannt ist, wo diese sich gerade befinden um Verluste etc. zu entdecken?	Is there a proper inventory for all data carriers and storage media in place so that you know where they are and discover losses immediately?
2-11		Gibt es ein Verfahren zur Datenlöschung im Sinne der DSGVO?	Is there a system for deletion of data according to GDPR in place?
2-12		Erfolgt die Entsorgung von alten Datenträgern, Fehldrucken mit sensiblen Informationen etc. auf einem sicheren Weg?	Do you dispose of old data carriers and storage media, printouts, faulty printouts and sensitive information in as safe way?
2-13		Gibt es eine interne Regelung für das Kopieren von Datenträgern? (z.B. Wer darf, wer nicht, …)	Is there an internal system in place that regulates authority to copy data carriers and storage media (who is allowed to, who is not)?
2-14		Gibt es schriftliche Regelungen für den Umgang mit mobile Devices (USB-Sticks, externe Festplatten, Tablets, Smartphones)?	Are there internal rules on the use mobile devices, such as USB sticks, external hard disks, tablets or smart phones in place?
2-15		Ist die Fernwartung von Servern und PCs so geregelt, dass Sie entweder über einen Verarbeitervertrag verfügen oder jederzeit Fernwartungen nachvollziehen können und die Geheimhaltung durch den Dienstleister sichergestellt ist?	Concerning remote maintenance of servers and computers, do you have a proper contract with the service provider that contains clauses on confidentiality and can you at any time retrace which maintenance activities were conducted?

3		**Regelungen zur Weitergabe von Daten und Zugängen**	**Rules on disclosure of data and access to data**
3-1		Ist ein sicherer Transport analoger Datenträger sichergestellt? (Boten, Post, etc.)	Did you make sure that data carriers and storage media is transported securely? (couries, post)?
3-2		Ist ein sicherer elektronischer Datenversand sichergestellt? (z.B. Anhänge in E-Mails)	Did you make sure that electronically transferred data in the form of e-mail attachments is safe?
3-3		Erfolgt die Auswahl von Auftragnehmern mit Zugriffsberechtigungen unter Berücksichtigung der DSGVO bzw. deren Qualifikation zur Einhaltung der DSGVO?	If you select external service providers who will have access to your data, do you assess their ability to respect the rules of GDPR?
3-4		Erfolgt die Weitergabe von Zugriffsberechtigungen an Subunternehmen im Sinne der DSGVO?	If you forward data or allow external service providers access to data, do you ensure compatibility with GDPR?

3-5		Gibt es eine schriftliche Regelung für Auftragnehmer mit Datenzugang im Sinne der DSGVO (Geheimhaltungsvereinbarung oder Verarbeitervertrag)?	Is there a written procedure for external service providers with access to data in place that regulates privacy and handling of data?
3-6		Werden Kontrollmaßnahmen durch eine/einen Datenschutzkoordinatorin/en durchgeführt?	Does your data protection officer conduct regular checks?

4		**Regelungen zur Umsetzung einer "Datensicherung" zzgl. Datensicherheit**	**Rules on Backups and Cyber Security**
4-1		Sind Brandschutz- und Wasserschutzmaßnahmen vorhanden?	Are protections against fire and floods in place?
4-2		Verfügen Sie über eine unterbrechungsfreie Stromversorgung für neuralgische IKT Geräte? (USV)	Do you have uninterruptible power supply for critical ICT devices in place?
4-3		Werden Sicherungsdatenträger sicher und störungsfrei aufbewahrt?	Are backup media stored safe and protected against incidents?
4-4		Wurden Backup-Verfahren eingeführt, die den Anforderungen des Betriebes entsprechen?	Do you have backup procedures according to the needs of your company in place
4-5		Ist der Einsatz von Cloud-Lösungen geregelt und sind Sie sich der damit verbundenen Sicherheitsrisiken bewusst?	Are there procedures on the use of cloud solutions in place and are you aware of possible security risks?
4-6		Ist ein Virenschutz auf allen Geräten eingeführt?	Is there a virus protection in place for all devices?
4-7		Erfolgen Funktionstests und Überprüfungen der Wiederherstellbarkeit des Backups?	Do you regularly test backup functions and recoverability?
4-8		Gibt es einen Notfallplan für externe (oder interne) Angriffe oder für Extremsituationen wie Schäden durch Feuer, Wasser etc. um eine Weiterführung des Betriebes sicher zu stellen?	Is there an emergency plan in place for disturbances such as cyber attacks, fire, floods etc in order to ensure that you can carry on the company?

Toolbox KMU.DIGITAL 2.0
IT-Security – bilingual checklist

Developed by WKÖ – Austrian Federal Economic Chamber
Translation: EUROCHAMBRES Digital Services Network

5	Regelungen der organisatorischen Datenschutz- und Sicherungsmaßnahmen	Internal Procedures concerning Data Protection and Data Security
5-1	Gibt es innerbetriebliche Regelungen zur Datensicherheit?	Do you have internal procedures on data security?
5-2	Gibt es ein IT-Sicherheitskonzept (Richtlinien, Arbeitsanweisungen, etc.)?	Do you have an IT security concept (directives, instructions for employees)?
5-3	Sind die organisatorischen Maßnahmen zum Schutz personenbezogener Maßnahmen konform mit der Datenschutz-Grundverordnung?	Are the organisational procedures concerning the protection of personal data compliant with the GDPR?
5-4	Erfolgt eine interne Kontrolle der Datenverarbeitungen?	Are there regular internal checks on the processing of data?
5-5	Die stichprobenartige Überprüfung von Protokollen und Login-Daten erfolgt regelmäßig durch einen Professionisten?	Are there regular random checks of the logs (data protocol) and login data by a qualified professional?
5-6	Ist die Vertretung von mit der EDV befassten Mitarbeiter/innen im Urlaub- und Krankheitsfall geregelt?	Is there a procedure in place for the substitution of the IT responsible in case of a sick leave or holidays?
5-7	Sind Ihre elektronischen Zutrittssysteme separat abgesichert? (z.B. Schlüsselkarten, etc.)	Are electronic access systems separately secured? (keycards, electronic door locks etc)

6	Regelung der externen/internen IT-Betreuung	Rules for internal/external IT support
6-1	Verfügt der Dienstleister/Mitarbeiter über Qualifizierungsnachweise (Zertifikate z.B. incite, WIFI, …)?	Does the IT responsible have the certificates proving he/she has the necessary qualifications?
6-2	Gibt es Vertretungsregelungen oder Notfallvorsorgen für den Fall der Nichtverfügbarkeit des Admins?	Is there a procedure in place for the substitution of the IT responsible or administrator in case of an emergency?
6-3	Werden bei der Beendigung der Tätigkeit als IT-Administrator dessen Zugangsmöglichkeiten gesperrt?	Are all access and rights of the IT responsible blocked if he/she leaves the company?

6-4		Gibt es dokumentierte Regelungen für Wartungs- und Reparaturarbeiten?	Are there written procedures in place concerning maintenance and repair?
6-5		Sind die Administrations-Kennungen (Benutzerdaten und Kennwörter) vor Zugriffen Dritter geschützt?	Are all admin credentials (identity and passwords) of the administrator secured against unwanted access by third party?
6-6		Wird Ihr System mittels Monitoring-Systeme (MDM) überwacht?	Is there a monitoring system for your IT in place?
6-7		Ist der Administrator für die laufende Aktualisierung der Dokumentation verantwortlich?	Does the administrator have a clear responsibility to record all maintenance activities?
6-8		Wurden "Auto-Update-Mechanismen" aktiviert/eingerichtet?	Have „auto-update“ functions been established or activated?

7		**Regelungen zum Schutz von WLANs**	**Rules on the Protection of the Wi-Fi**
7-1		Erfolgte nachweislich eine sichere Basiskonfiguration Ihres Accesspoints oder WLAN-Routers (Einhaltung der WLAN-Sicherheitsstandards)?	Is there verifiable evidence that the basic configuration of the Wi-Fi access point is secure? (compliance with Wi-Fi security standards)
7-2		Ist sichergestellt, dass die Mitarbeiter/innen das betriebliche WLAN mit privaten Geräten nicht benutzen können?	If the internal Wi-Fi allows access to corporate data, did you make sure that employees cannot use company Wi-Fi with their private devices?
7-3		Ist sichergestellt, dass Gäste/Besucher/private Endgeräte in einem separaten WLAN abgetrennt werden und so keinen Zugriff auf Unternehmensdaten haben?	Did you make sure that guests or private devices log into a separate Wi-Fi and are therefore never connected to the company Wi-Fi?
7-4		Sind Ihre Mitarbeiter/innen darauf geschult, die Zugangsdaten des WLANs nicht an Dritte weiter zu geben?	Have employees been trained/advised to never disclose login information of the company Wi-Fi to thirds?
7-5		Führen Sie eine regelmäßige Überprüfung der im WLAN angemeldeten Benutzer und Endgeräte durch?	Are there regular checks on which devices are connected to the Wi-Fi?

Toolbox KMU.DIGITAL 2.0
IT-Security – bilingual checklist

Developed by WKÖ – Austrian Federal Economic Chamber
Translation: EUROCHAMBRES Digital Services Network

8		Regelungen zur sicheren Einrichtung einer Firewall	Rules on the secure establishment of a firewall
8-1		Ist eine sichere Grundkonfiguration dieser Firewall dokumentiert und sichergestellt?	Is there verifiable evidence that the firewall is updated and patched?
8-2		Werden regelmäßig Updates und Patches (Firmware) auf dem Gerät eingespielt?	Are there regular updates including importing patches (firmware)?
8-3		Ist die Administrationsschnittstelle geschützt?	Is the firewall management interface properly protected?
8-4		Erfolgt die Absicherung von grundlegenden Internetprotokollen?	Are the basic internet protocols properly secured?
8-5		Haben Sie geeignete Filterregelungen am Paketfilter eingerichtet?	Have you set suitable filter rules for the firewalls?
8-6		Sind Reaktionszeiten für den Fall des Ausfalles der Firewall mit internem Personal bzw. externen Dienstleistern geregelt?	Have you determined the reaction times with your employees or external service provider in case your firewall is down?
8-7		Wurde eine Betriebsdokumentation erstellt und wird diese laufend aktualisiert?	Are there log books or documentations for the firewalls and are they updated regularly?

9		Regelungen zum Schutz von Fernzugriffen	Rules on Secure Remote Access
9-1		Ist ein externer Zugriff mittels VPN (Virtual Private Network) eingerichtet?	Is an external access via VPN (Virtual Private Network) set up?
9-2		Wurde eine Sicherheitsrichtlinie zur VPN-Nutzung erstellt?	Did you put security guidelines for VPN in place?
9-3		Werden nicht mehr benötigte VPN-Zugänge gesperrt?	Did you disable all old VPN accounts that are no longer used?
9-4		Werden Zugriffsvorgänge über die VPN-Zugänge protokolliert und regelmäßig geprüft?	Are there records for the VPN accounts and are they updated regularly?

Toolbox KMU.DIGITAL 2.0
IT-Security – bilingual checklist

Developed by WKÖ – Austrian Federal Economic Chamber
Translation: EUROCHAMBRES Digital Services Network

10	Regelungen zur Schulung von Mitarbeiter/innen	Rules on Staff Training
10-1	Sind Reaktionen auf Verletzungen der Sicherheitsvorgaben in Ihrem Betrieb definiert und geschult?	Did you define and provide training for your staff concerning the consequences and responses in case of non-compliance with security rules?
10-2	Werden Fremdpersonen in sensiblen Bereichen beaufsichtigt und begleitet?	Do you accompany guests in sensitive areas of your premises?
10-3	Erfolgt eine geregelte (dokumentierte) Einarbeitung/Einschulung neuer Mitarbeiter/innen?	Is there a procedure for training of new staff and records on such training in place?
10-4	Haben Sie eine Rollenbeschreibung der Arbeitsplätze?	Do you have job descriptions of positions in place?
10-5	Gibt es eine geregelte (dokumentierte) Verfahrensweise beim Weggang eines Mitarbeiters/einer Mitarbeiterin?	Is there a documented procedure when an employee leaves the company?
10-6	Werden Ihre Mitarbeiter/innen regelmäßig auf IT-sicherheitsrelevante Verfahren geschult?	Do you provide regular trainings for employees on IT security procedures?
10-6a	Werden Ihre Mitarbeiter/innen regelmäßig auf die Abwehr potenzielle IT-sicherheitsrelevanter Angriffe (insb verdächtige Mails, Phishing, Vorgabe falscher Identitäten in elektronischen Nachrichten etc) geschult?	Do you provide regular trainings for employees on to prevent potential attacks related to IT security (especially suspicious e-mails, phishing, use of false identities in electronic messages, etc)?
10-7	Erfolgt eine Sensibilisierung Ihrer Mitarbeiter/innen hinsichtlich Informationssicherheit?	Are you regularly raising awareness for IT security issues among your employees?
10-8	Werden Ihre Mitarbeiter/innen im sicheren Umgang mit IT-Systemen geschult?	Do you provide regular trainings for employees on secure handling of IT systems?
10-9	Gibt es eine schriftliche Richtlinie zur sicheren IT-Nutzung?	Do you provide written guidelines on secure handling of IT systems?
10-10	Gibt es Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal? (inkl. Putzpersonal)	Are there confidentiality agreements for external service providers in place (including cleaning staff)?
10-11	Haben Sie eine schriftliche Verschwiegenheits-/Vertraulichkeitsvereinbarung mit Ihren Mitarbeiter/innen?	Are there written confidentiality agreements for staff in place?

Toolbox KMU.DIGITAL 2.0
IT-Security – bilingual checklist

Developed by WKÖ – Austrian Federal Economic Chamber
Translation: EUROCHAMBRES Digital Services Network

11	Regelungen zum Umgang mit mobilen Endgeräten		Rules on Mobile Devices
11-1		Ist eine sichere Grundkonfiguration für mobile Geräte sichergestellt?	Did you make sure that the basic configurations of the mobile devices are secure?
11-2		Ist die Verwendung eines erweiterten Zugriffsschutz (Passwort statt PIN) sichergestellt?	Is the use of an extended access protection (password instead of the PIN) ensured?
11-3		Erfolgen regelmäßige Updates von Betriebssystem und Applikationen?	Are there regular updates of operating systems and applications taking place?
11-4		Wurden nichtbenutzte Kommunikationsschnittstellen deaktiviert (Ortungsdienste, ...)?	Were all unused data access point deactivated, such as GPS tracking systems?
11-5		Gibt es schriftliche Richtlinien zur Benutzung von betrieblichen Mobilen Endgeräten?	Are there written regulations for the use of the company's mobile devices in place?
11-6		Ist die Auswahl und Freigabe von Applikationen vor der Installation sichergestellt?	Is the selection and approval of applications ensured before installation?
11-7		Gibt es eine Definition von erlaubten Informationen (Dateien, Kontakte, E-Mail-Konten) auf mobilen Geräten?	Did you define which information may be stored on mobile devices (files, contacts, e-mail accounts)?
11-8		Ist sichergestellt, dass bei betrieblicher Nutzung von privaten Endgeräten eine explizite/schriftliche Regelung vorliegt?	Are there written regulations for the use of private mobile devices for company purpose in place?
11-9		Nutzen Sie zur Verwaltung der (betrieblichen) mobilen Endgeräte ein Mobile-Device- Management (MDM)?	Do you use a mobile device management system for the administration of your mobile devices?
11-10		Ist die Nutzung von privaten Endgeräten für betriebliche Zwecke erlaubt? (Dulden = erlauben)	Do you in your company allow the use of private mobile devices for company purposes? (If management does not explicitly forbid the use of private mobile devices for company purposes it is considered to be tolerated)
11-11		Verwenden Sie auf dem mobilen Endgerät einen lokalen Virenschutz?	Do you use a virus protection programme for each mobile device?
11-12		Ist die "automatische Sperre" in den Einstellungen aktiviert?	Is the auto-lock function activated for all mobile devices?
11-13		Ist die Möglichkeit einer Fernlöschung sichergestellt?	Did you make sure that you can delete data remotely?