



ARBEITSANWEISUNG FÜR ANGESTELLTE MIT PRIVATGERÄTEN

ISTRUZIONI DI LAVORO PER DIPENDENTI CON DISPOSITIVI PROPRI

Diese Arbeitsanweisung soll dazu beitragen, dass die Rechtsvorschriften zur Verarbeitung personenbezogener Daten und zum Schutz der informationstechnischen Systeme eingehalten werden und insbesondere die Vertraulichkeit, Integrität und Verfügbarkeit von betrieblichen/geschäftlichen Dokumenten und Informationen sowie damit zusammenhängenden personenbezogenen Daten gewährleistet werden kann, sowohl am Arbeitsplatz im Büro als auch im Homeoffice.

Le presenti istruzioni di lavoro hanno lo scopo di contribuire a garantire il rispetto delle disposizioni di legge sul trattamento dei dati personali e della sicurezza informatica e, in particolare, che possa essere garantita la riservatezza, l'integrità e la disponibilità di documenti e informazioni aziendali/d'ufficio e dei collegati dati personali, sia sul posto di lavoro in ufficio, sia in sede di telelavoro.

Anwendbare Normen: Verordnung (EU) 2016/679, Art. 32, sowie Vorgaben der Autorità Garante per la protezione dei dati personali

Präventionsrichtlinien der ENISA

Präventionsrichtlinien von EUROPOL

Norme applicabili: Regolamento (UE) 2016/679, Art. 32, nonché specifiche dell'Autorità Garante per la protezione dei dati personali

Linee guida ENISA

Linee guida EUROPOL

1. VORGABEN PRIVATGERÄTE

1. DIRETTIVE PER L'UTILIZZO DI DISPOSITIVI PROPRI

UPDATES

1.1. PCs und Laptops müssen mit einem aktiven und aktuellen Antivirenprogramm ausgestattet sein.

Die Betriebssysteme und Programme auf PCs und Laptops sind immer auf dem aktuellen Stand zu halten. Mit Updates werden meist Sicherheitsschwachstellen behoben.

PASSWÖRTER

1.2. Starke Passwörter schützen Systeme und Daten vor dem Zugriff durch Unberechtigte. Die Passwörter müssen den gängigen Sicherheitsstandards entsprechen.

UPDATES

1.1. PC e PC portatili/laptops devono essere dotati di antivirus attivo ed aggiornato.

I sistemi operativi e i programmi su PC e PC portatili/laptops devono essere sempre tenuti aggiornati. Gli aggiornamenti vengono solitamente utilizzati per correggere le vulnerabilità della sicurezza.

PASSWORD

1.2. Password complesse proteggono sistemi e dati da accessi non autorizzati. Le password devono corrispondere agli standard attuali.

2. NUTZUNG DER VPN-VERBINDUNG

2. UTILIZZO DELLA CONNESSIONE VPN

VERBINDUNG

2.1 Für die Verbindung mit dem Computernetzwerk der Gemeinde, muss die vom Gemeindevorstand zur Verfügung gestellte VPN-Software verwendet werden;

CONNESSIONE

2.1 Per il collegamento alla rete informatica della comune deve essere utilizzato il software VPN messo a disposizione dal Consorzio dei Comuni;

2.2 Der Zugang erfolgt über LDAP-Benutzername und Passwort;

2.3 Die Berechtigung für den Zugriff über VPN wird vom EDV-Verantwortlichen erteilt;

SICHERE IDENTIFIKATION

2.4 Die im vorhergehenden Punkt beschriebenen Zugriffe sind als streng persönlich einzustufen und die entsprechenden Passwörter dürfen niemals an Dritte weitergegeben werden.

2.2 L'accesso avviene tramite nome utente e password LDAP;

2.3 L'abilitazione all'accesso tramite VPN viene data dal responsabile EDP;

IDENTIFICAZIONE SICURA

2.4. Gli accessi descritti al punto precedente sono da intendersi come strettamente personali e le relative password non devono mai essere comunicate a terzi.

3. WEITERE VORGABEN

GESCHÄFTLICHE DOKUMENTE, INFORMATIONEN UND PERSONENBEZOGENE DATEN SCHÜTZEN

3.1. Dokumente, Informationen und personenbezogene Daten sind zu schützen, auch im Homeoffice:

- die Inhalte des/r vom Arbeitgeber/Verantwortlichen erteilten Auftrags und Anweisungen gemäß Art. 29 EU-Verordnung Nr. 679/2016 für die Verarbeitung von personenbezogenen Daten sind auch im Zuge der Verwendung von Privatgeräten einzuhalten;
- Zugangspasswörter sind geheim zu halten;
- Interne Informationen und personenbezogene Daten sind vor Unberechtigten, auch Familienmitgliedern, zu schützen;
- Der Bildschirm ist vor Einsicht zu schützen;
- Auf dem privaten Gerät sind keine Dokumente, Informationen und personenbezogenen Daten zu speichern;
- Papierdossiers und Ausdrücke sind vor unberechtigtem Zugriff zu schützen;
- Nicht mehr benötigte Papierunterlagen sind zu schreddern oder sicher aufzubewahren, bis sie im Büro vernichtet werden können.

E-MAIL SICHER EINSETZEN

3.2. Private und geschäftliche E-Mails sind auf dem Gerät zu trennen. Die Nutzung privater E-Mail-Konten für die geschäftliche Kommunikation ist verboten. Geschäftliche E-Mails dürfen nicht auf private Konten weitergeleitet werden.

KOMMUNIKATIONS-TOOLS AUSWÄHLEN

3.3. Neben dem Telefon und den E-Mails werden auch Messengers und Videokonferenzdienste eingesetzt. Informationen zu den Diensten erhalten Sie auf Anfrage beim IT-Verantwortlichen.

3. ALTRE PRESCRIZIONI

PROTEGGERE I DATI PERSONALI E SEGRETI D'UFFICIO (DOCUMENTI, INFORMAZIONI)

3.1. Documenti, informazioni e dati personali devono essere protetti, anche durante il telelavoro:

- I contenuti dell'incarico e delle istruzioni del datore di lavoro/Titolare di trattamento ex art. 29 regolamento UE n. 679/2016 per il trattamento dei dati personali sono da rispettare anche nell'utilizzo dei dispositivi propri;
- Le password di accesso devono essere tenute segrete;
- Le informazioni interne e i dati personali devono essere protetti da persone non autorizzate, compresi i familiari;
- Lo schermo deve essere protetto dalla vista di terzi,
- Sul dispositivo privato documenti, informazioni e dati personali non devono mai essere salvati;
- I fascicoli cartacei e le stampe devono essere protetti dall'accesso non autorizzato;
- I documenti cartacei non più necessari devono essere distrutti o conservati in un luogo sicuro fino a quando non possono essere distrutti in ufficio;

UTILIZZO SICURO DELLE MAIL

3.2. Le e-mail private e aziendali devono essere separate sul dispositivo. È vietato utilizzare account di posta elettronica privati per la comunicazione aziendale. Le e-mail aziendali non devono essere inoltrate ad account personali.

SELEZIONE MIRATA DEGLI STRUMENTI DI COMUNICAZIONE

3.3. Oltre al telefono e alla posta elettronica, vengono utilizzati anche servizi di messaggistica e videoconferenza. Le informazioni sui servizi sono disponibili su richiesta presso il responsabile del reparto informatico.

SICH VOR PHISHING UND ANDEREN BEDROHUNGEN SCHÜTZEN

3.4. Verdächtige E-Mails dürfen nicht geöffnet werden. Anhänge in Mails von unbekanntem Absender dürfen nicht angeklickt werden. Im Zweifel ist die Absenderin oder der Absender per Telefon zu kontaktieren, damit sie oder er den Inhalt der E-Mail bestätigen kann.

DATENSCHUTZVERLETZUNGEN SOFORT MELDEN

3.5. Wenn Arbeitsmittel wie Dokumente oder auch Ihr PC oder Laptop verloren gehen oder abhanden kommen, ist dies umgehend dem Vorgesetzten zu melden.

Zusätzliche Informationen zum Thema IT-Sicherheit im Privathaushalt finden Sie unter: <https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold>

PROTEGGETEVI DAL PHISHING E DA ALTRE MINACCE

3.4. Le e-mail sospette non devono essere aperte. Non fare clic sugli allegati nelle e-mail di mittenti sconosciuti. In caso di dubbio, il mittente deve essere contattato telefonicamente in modo che possa confermare il contenuto dell'e-mail.

SEGNALARE IMMEDIATAMENTE I DATA BREACH

3.5. In caso di smarrimento di documenti oppure del PC/PC portatile laptop è necessario segnalarlo immediatamente al responsabile di reparto.

Altre informazioni riguardanti la sicurezza informatica a casa Vostra trovate sotto: <https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold>

4. KONTROLLEN

4.1. Die Tätigkeiten der Mitarbeiter für den Arbeitgeber/Verantwortlichen, welche mittels Privatgeräten abgewickelt werden, werden nicht systematisch und kontinuierlich überwacht, die Systemadministratoren des Arbeitgebers/Verantwortlichen (auch in Zusammenarbeit mit der EDV-Abteilung) können die Tätigkeiten auf den Servern des Arbeitgebers/Verantwortlichen (z.B. die erzeugten Logfiles; die Privatgeräte selbst werden klarerweise nicht kontrolliert) aber überwachen oder untersuchen; dies geschieht nur, um die Einhaltung der relevanten Richtlinien zu bestätigen und mögliche Sicherheitsverletzungen, unbefugte Zugriffe, technische Probleme, usw. zu untersuchen und nicht für die Zwecke der Überwachung der Arbeitstätigkeit. Die Verwendung von Logfiles erfolgt immer mit einer festgelegten zeitlichen Begrenzung (kurze Frist) und Tracing-Tätigkeit erfolgt nur bei allfälligen Verdachtsmomenten, in manueller Form und üblicherweise in direkter Zusammenarbeit mit dem betroffenen Nutzer.

Die Kontrollen können wie folgt zusammengefasst werden:

- 1) Kontrolle/Einschränkung auf der Grundlage der IP der Region, aus welcher der Verbindungszugriff erfolgt (ev. auch für weitere Dienste)
- 2) Kontrolle/Einschränkung auf der Grundlage der IP für den E-Mail-Zugang
- 3) Befähigung bestimmter IP's in Zusammenhang mit kritischen Diensten (z.B. Meldedaten an die Polizeikräfte)
- 4) zusätzliche Kontrollformen, die im Laufe der Zeit,

4. VERIFICHE

4.1 Le attività dei dipendenti, svolte per datore di lavoro/Titolare utilizzando dispositivi propri, non sono soggetti a una sorveglianza sistematica e continua, ma gli amministratori di sistema del datore di lavoro/Titolare (anche in collaborazione con la Ripartizione CED) possono monitorare o indagare le attività sui server del datore di lavoro/Titolare (p.es. i logfiles generati; i dispositivi propri in sé ovviamente non vengono controllati); ciò si verificherà solo per confermare la conformità ai requisiti della politica pertinente e per indagare su possibili violazioni della sicurezza, accessi non autorizzati, problemi tecnici, ecc. e non ai fini del monitoraggio dell'attività lavorativa. L'utilizzo di logfiles è limitato a tempistiche prefissate (breve termine) e l'attività di tracing viene espletata solo nei casi di dubbio, in forma manuale e di regola in collaborazione diretta con l'utente interessato.

Le attività di controllo possono essere così riassunte:

- 1) controllo/restrizione su base IP della regione di accesso per collegamento VPN (ev. anche per altri servizi)
- 2) controllo/restrizione su base IP per l'accesso alle e-mail
- 3) abilitazione su IP specifici dei servizi critici (es. anagrafe alle forze dell'ordine)
- 4) ulteriori forme di controllo che costituiranno, nel continuo, la best practice di settore (p.es.

zur best practice des Sektors zählen werden (z.B. conditional access und multifactor authentication, usw.)

conditional access e multifactor authentication, ecc.)

5. RECHT AUF NICHTERREICHBARKEIT

5. DIRITTO ALLA DISCONNESSIONE

Im Fall von Telearbeit/Smartworking sieht die individuelle Vereinbarung zwischen Arbeitgeber und Angestellten u.a. die Ruhepausen mit Anrecht auf Unterbrechung der Verbindung vor.

In caso di telelavoro/smartworking l'accordo individuale tra il datore di lavoro e il dipendente prevede, tra l'altro, i tempi di riposo con diritto alla disconnessione;