ARI
Appenzell Ausserrhoden
Informatik

Appenzell Ausserrhoden
Datenschutz-
Kontrollorgan

Tipps für ein sicheres Homeoffice

(Hinweis: Mit Homeoffice sind hier alle Arbeiten von zu Hause aus oder unterwegs gemeint)

Benutzer der IT-Infrastruktur der AR Informatik AG (ARI) sind auch im Rahmen des Homeoffice für die Einhaltung der gesetzlichen Vorschriften und internen Weisungen (insb. Datenschutz und Datensicherheit) verantwortlich. Die nachfolgenden Tipps für einfache und zweckmässige Massnahmen sollen dabei helfen.

1. Geheimhaltungspflicht
Auch im Homeoffice sind Sie verpflichtet, Unterlagen mit vertraulichem Inhalt o.ä., die für die Erfüllung der Arbeitspflicht benötigt werden, geheim zu halten. Sie dürfen nicht unbeaufsichtigt am Arbeitsplatz liegen gelassen werden oder Dritten, einschliesslich Familienmitgliedern, in irgendeiner Form zugänglich gemacht werden. Werden keine Homeoffice-Arbeiten verrichtet, sind Unterlagen mit vertraulichem Inhalt o.ä. in einem verschliessbaren Schrank aufzubewahren oder auf andere Weise der Zugriff für Dritte zu verhindern. Der für geschäftliche Zwecke genutzte Computer ist mit einem Passwortschutz zu versehen. Dies gilt auch für geschäftlich genutzte Privatgeräte.

2. Umgang mit Arbeitsmitteln
Die zur Verfügung gestellten Arbeitsmittel sind mit der erforderlichen Sorgfalt zu benutzen. Arbeitsmittel dürfen nicht Dritten, einschliesslich Familienmitgliedern, überlassen werden. Fenster und Türen sind abzuschliessen, wenn des Homeoffice-Platz nicht besetzt ist (z.B. beim Verlassen des Hauses, der Wohnung oder des Hotelzimmers). Generell muss sichergestellt sein, dass Unbefugte zu keiner Zeit auf geschäftliche IT-Systeme und Unterlagen zugreifen können. Der häusliche Arbeitsplatz muss aufgeräumt hinterlassen werden und es dürfen keine sensitiven Informationen frei zugänglich sein.

3. Sicherheitstechnische Anforderungen an die für das Homeoffice eingesetzten IT-Systeme
Zur Minimierung der Angriffsfläche müssen die für das Homeoffice verwendeten IT-Systeme gehärtet sein. Dies bedeutet, dass insbesondere bei der Verwendung privater Geräte darauf geachtet wird, dass von den Mitarbeitenden laufend aktuelle Software-Patches und Antivirus-Signaturen eingespielt werden und die Personal Firewall nicht deaktiviert wird. Bei von ARI zur Verfügung gestellten IT-Geräten erfolgt dies automatisch.

4. Sicherer Remote-Zugriff auf das Firmen-Netz
ARI stellt für den Zugang ins Firmen-Netz verschiedene, sichere Möglichkeiten zur Verfügung. Nützen Sie ausschliesslich die von ARI zur Verfügung gestellten Zugriffsmöglichkeiten und beachten Sie insbesondere die entsprechenden Installationsanweisungen. Über öffentlich zugängliche Netze (z.B. Public W-LAN) darf nur über einen sicheren Kommunikationskanal (z.B. verschlüsseltes VPN) auf interne Ressourcen zugegriffen werden. Eine externe Verbindung hat immer über eine 2-Faktor-Authentifizierung (SMS, Authenticator-App oder privates E-Mail) zu erfolgen.

5. Datensicherung
Bei mobilen IT-Systemen ist die Gefahr der Zerstörung durch Stürze, Schäden durch Transport, ungünstige klimatische Bedingungen sowie falsche Aufbewahrung wesentlich grösser, als bei einem stationären Arbeitsplatz. Auch ein Verlust durch Diebstahl oder einfaches „Liegen lassen" kommt häufig vor. Daher sollte eine regelmässige Datensicherung der lokal gespeicherten Daten durchgeführt werden (z.B. durch regelmässiges Sichern bearbeiteter, offener Dokumente). Wichtige Daten dürfen nicht lokal gespeichert werden. Sollte dies trotzdem erforderlich sein, muss die Sicherung auf verschlüsselten Datenträgern erfolgen und eine Kopie der Daten auf dem Firmennetz abgelegt werden.

6. Meldepflicht im Verlust-/Schadensfall
Tritt bei Verrichtung von Homeoffice-Arbeit ein Verlust- oder Schadensfall geschäftlich genutzter IT-Mittel ein, ist dies unverzüglich dem Servicedesk von ARI zu melden (z.B. Diebstahl oder Verlust eines Laptops, Smartphones oder USB-Sticks mit geschäftlichen Daten). Nur so kann ARI zeitnah mit Massnahmen wie das Ändern von Passwörtern oder das Sperren von Zugängen reagieren.

7. Support für Homeoffice-Arbeitsplätze
Falls Sie Support bei der Verwendung von Homeoffice-Infrastruktur benötigen, konsultieren Sie bitte die zur Verfügung gestellten Anleitungen auf der öffentlich zugänglichen Internet-Seite http://www.ari-ag.ch/homeoffice. Sollten Sie weiteren Support benötigen, kontaktieren Sie bitte das Servicedesk von ARI unter servicedesk@ari-ag.ch oder 071 353 94 44.

8. Entsorgung von vertraulichen Informationen
Informationen (z. B. Datenträger und Dokumente) sind in geeigneter Weise zu entsorgen und dürfen auf keinen Fall in den Hausmüll geworfen oder unterwegs unsachgemäss entsorgt werden. Bevor ausgediente oder defekte Datenträger und Dokumente weggeworfen werden, muss überprüft werden, ob sie sensible Informationen enthalten. Ist dies der Fall, müssen die Datenträger und Dokumente wieder ins Geschäft zurücktransportiert und gemäss den internen Vorschriften auf sichere Art und Weise entsorgt bzw. vernichtet werden.

9. Vorsicht Phishing!
Gerade in Krisenzeiten können vermehrt Phishing E-Mails auftreten, die die aktuelle Situation ausnutzen wollen und versuchen, an sensible Daten mit Hinweis auf Remote-Zugänge, das Zurücksetzen von Passwörtern etc. zu gelangen. Wie Sie Phishing-Versuche erfolgreich erkennen können, erfahren Sie z.B. auf der Webseite von iBarry: https://www.ibarry.ch/de/risiken-im-internet/phishing/.

ARI
Appenzell Ausserrhoden
Informatik
Service Desk
Montag bis Freitag, 07:00 bis 17:00 Uhr
AR Informatik AG
Poststrasse 10a
9102 Herisau
Tel. 071 353 94 00
info@ari-ag.ch

Appenzell Ausserrhoden
Datenschutz-Kontrollorgan
Poststrasse 23
9001 St. Gallen
Stefan Gerschwiler
lic. iur., Rechtsanwalt
Tel. 071 228 29 30
stefan.gerschwiler@ar.ch