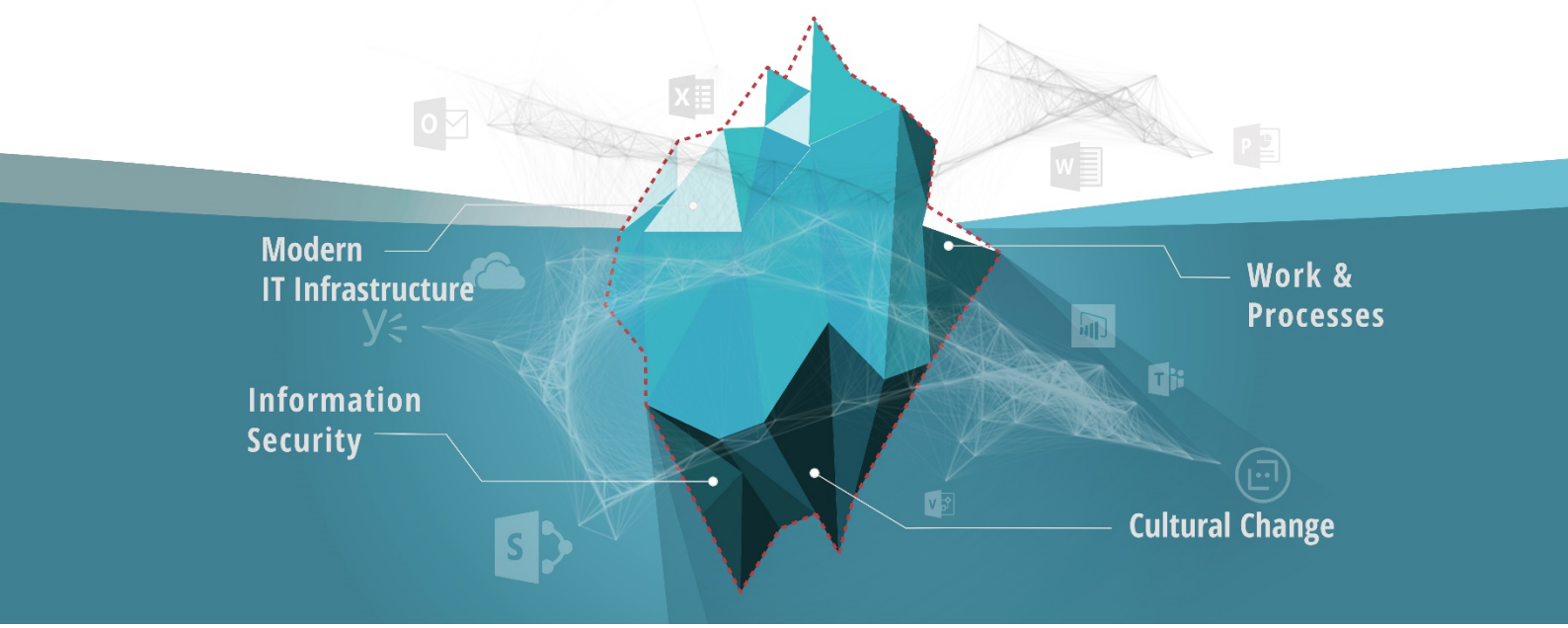

Vorlage ISMS Richtlinie zu Home-Office und Telearbeit

Für die Kommunikation an Ihre Mitarbeiter

Die Inhalte der nachfolgenden Information (ab Seite 2) können Sie gerne kopieren, anpassen und für Ihre Mitarbeiterkommunikation einsetzen. Das daraus entstehende Dokument hat das Ziel die Home-Office- und Telearbeit zu regeln. Daneben unterstützten die enthaltenen Sicherheitsmaßnahmen beim Schutz von Informationen, auf die mobil zugegriffen, die verarbeitet oder gespeichert werden.

Sind Ihre Daten sicher? Sicher?
Eine Schutz- und Risikoanalyse bietet weitere Informationen, welche Maßnahmen am digitalen Arbeitsplatz und im Home-Office erforderlich sind, um sicheres Arbeiten zu gewährleisten. Mehr Informationen zum Schutz Ihrer Daten auf www.adlon.de/digital-workplace/information-security

Inhalte der Schutz- und Risikoanalyse, Übersicht zu:

- Ihren sicherheitsbedürftigen Daten
- sensiblen Prozesse
- Zusammenhänge Ihrer Systeme und Prozesse
- dem Sicherheitsbewusstsein Ihrer Mitarbeiter
- Haftung und Verantwortung im Schadensfall

ADLON Intelligent Solutions GmbH
ADLON gestaltet als IT-Beratungsunternehmen Ihren Digital Workplace ganzheitlich.
Dazu gehört auch die Entwicklung des fortlaufenden Prozesses der Informationssicherheit.

Kontakt:
ADLON Intelligent Solutions GmbH | Albersfelder Straße 30 | 88213 Ravensburg
Telefon-Nr. +49 751 7607-70 | zentrale@adlon.de | www.adlon.de/home-office

KOPIERVORLAGE

ISMS Richtlinie zu Home-Office und Telearbeit

[Firma]

Inhaltsverzeichnis

1 Allgemeines

1.1 Dokumentenlenkung

1.1.1 Adressaten

Das vorliegende Dokument gilt für alle Mitarbeiter und für den Anwendungsbereich des Informationssicherheits-Managementsystems ISMS der [Organisationsname] (im Folgenden „[Organisationsname]“ genannt).

1.1.2 Änderungshistorie

Version	Datum	Änderung	Durchführung	Prüfung / Freigabe

1.1.3 Ziel und Zweck der Richtlinie

Das vorliegende Dokument gliedert sich in der Dokumentenhierarchie des ISMS ein und regelt das Arbeiten von Mitarbeitern per Telearbeit (im Folgenden „Arbeiten per Fernzugriff“ genannt) sowie den Umgang mit Telearbeitsplätzen (im Folgenden „Home-Office“ genannt), von denen aus [Organisationsname]-Mitarbeiter für die [Organisationsname] arbeiten können.

Diese Richtlinie regelt unterstützende Sicherheitsmaßnahmen zum Schutz von Informationen, auf die per Fernzugriff und/oder von Home-Offices aus zugegriffen wird oder die dort verarbeitet oder gespeichert werden.

1.1.4 Begriffsdefinition

Unter Telearbeit wird bei der [Organisationsname] jegliche Teilnahme am Arbeitsprozess über elektronische Medien durch interne und externe Mitarbeiter bezeichnet, die sich nicht in einer der Niederlassungen aufhalten. Beispiel für die Telearbeit kann hier die Arbeit in Zug, Auto, Flugzeug oder auch Public Workspaces sein.
Ein Home-Office ist ein fest installierter Arbeitsplatz außerhalb der Niederlassungen, von dem der Mitarbeiter aus regelmäßig und dauerhaft per Fernzugriff am Arbeitsprozess teilnimmt.

2 Telearbeit

2.1 Grundsätzlicher Zugriff

Der Fernzugriff auf das lokale Netzwerk der [Organisationsname] kann entweder über VPN auf SSL-Basis oder über das Citrix-Portal erfolgen.
VPN-Portal: https://sslvpn.[Organisationsname].org
Citrix-Umgebung: https://citrix.[Organisationsname].org

2.1.1 Endgeräte und Sicherheitsprüfung

Der Benutzer kann für die Telearbeit ein von der [Organisationsname] verwaltetes, dem Mitarbeitenden zur Verfügung gestelltes Endgerät nutzen. Diese Geräte müssen den aktuellen Mindestanforderungen der Compliance entsprechen. Ein Zugriff von Geräten, die nicht den Anforderungen der Compliance entsprechen, ist nicht möglich.

2.1.2 Authentifizierung

Mitarbeiter der [Organisationsname] nutzen für die Authentifizierung Ihrer Benutzerkennung neben ihrer Benutzerkennung, bestehend aus <Vorname.Nachname>, einen zweiten Faktor. Ohne diese Authentifizierung ist kein Zugriff auf Unternehmensressourcen der [Organisationsname] möglich.

Näheres zur Handhabung und der technischen Umsetzung von Passwörtern und der Zwei-Faktor-Authentifizierung regelt die eigene Richtlinie „Umgang mit Passwörtern“.

2.1.3 Zugriffsorte

Der Benutzer kann sich von einem Ort seiner Wahl mit dem VPN-Portal verbinden. Grundsätzlich hat er jedoch die Regelungen der Benutzerrichtlinie unter Ziffer 3.4 „Nutzung von Endgeräten in öffentlichen Räumen“ zu beachten. Dazu zählt ebenso, dass sichergestellt sein muss, dass auf dem Client keinerlei Software ausgeführt wird, welche die Verbindungsparameter oder deren Eingabe speichert (z. B. Browsercache, Keylogger).

2.2 Benutzerrechte

Grundsätzlich ist jeder Mitarbeiter der [Organisationsname] zur Nutzung des VPN-Portals sowie der Citrix Umgebung berechtigt. Die möglichen Zugriffe richten sich jedoch nach dem Bedarf und den vorab definierten Rechten des Mitarbeiters. Standardmäßig bietet sich dem Benutzer ein identischer Zugriff auf Ressourcen, wie wenn er sich in einer der Niederlassungen befindet.

2.3 Zugriff für externe Benutzer

Externe Dienstleister können ebenso einen individuell konfigurierbaren Zugriff erhalten. Hierfür wird im Benutzerverzeichnis ein Benutzeraccount mit dem Suffix .EXT angelegt. Für externe Benutzer ist eine Zwei-Faktor-Authentifizierung verpflichtend.

Zum Schutz von Unternehmensinformationen ist der Abschluss einer entsprechenden Zusatzvereinbarung mit dem externen Dienstleister zwingend erforderlich bevor der Zugriff freigeschaltet wird.
Zugriffe für externe Benutzer werden bei Bedarf aktiviert und im Rahmen eines dreimonatigen Reviews auf Gültigkeit und Bedarf geprüft.

2.4 Möglichkeiten der Sperrung des Fernzugriffs

Der Fernzugriff für Mitarbeiter und Dienstleiter kann jederzeit gesperrt werden. Dies erfolgt zentral durch Entfernen des Benutzers aus der Gruppe "VPN-User“.

3 Home-Office

3.1 Genehmigung

Die Genehmigung zur Einrichtung eines Home-Office erfolgt durch den jeweiligen Vorgesetzten, sowie in letzter Instanz durch die Geschäftsführung. Die Häufigkeit der Nutzung sowie die Arbeitszeiten werden individuell im Arbeitsvertrag oder entsprechenden Zusatzverträgen geregelt. Ein Anspruch auf dauerhafte Verfügbarkeit oder Funktionalität hat der Mitarbeiter jedoch nicht.

3.2 Ausstattung

Home-Offices werden standardmäßig von [Organisationsname] mit folgenden Komponenten ausgestattet:

- Internetanschluss (Bandbreite und Anbindungsvariante variieren in Abhängigkeit der technischen Voraussetzung am Standort des Home-Office)
- Netzwerk-Anbindung
- Firewall
- Headset zur Telefonie über Microsoft Teams
- Von [Organisationsname] verwaltetes Endgerät, welches den aktuellen Anforderungen der Compliance entspricht

Die Einrichtung aller weiteren für die Arbeit des Mitarbeiters notwendigen und dafür geeigneten Arbeitsmittel (wie z.B. Arbeitstisch, Bürostuhl, Aufbewahrungsmöbel, Stromanbindung, etc.) übernimmt der Mitarbeiter in eigener Verantwortung und auf eigene Kosten.
Für von der [Organisationsname] zur Verfügung gestelltes Equipment gelten die entsprechenden Anweisungen in der Benutzerrichtlinie.

Am Home-Office gelten dieselben Arbeitssicherheitsrichtlinien wie am [Organisationsname]-Standort und sind vom Mitarbeiter einzuhalten.

3.3 Zutrittskontrolle im Home-Office

Ein Home-Office muss sich in einem festen Gebäude befinden, welches über die üblichen Sicherheitsmaßnahmen, wie z.B. verschließbare Fenster und Türen, verfügt. Üblicherweise wird ein Home-Office innerhalb der Wohnung bzw. Hauses des Mitarbeiters eingerichtet.

- Der Mitarbeiter verpflichtet sich, der [Organisationsname] bzw. der von dieser beauftragten Personen (insbesondere Dienstleister für den EDV-Support, Datenschutzbeauftragte), die auf Grund gesetzlicher Verpflichtungen Zugang zur häuslichen Arbeitsstätte haben müssen, Zugang zu dieser zu gewähren, soweit dies aus sachlichen Gründen erforderlich ist. Der Zutritt und Zugang ist ins-besondere zur Überprüfung der vertraglich vereinbarten Anforderungen an das Home-Office zu gewähren.
- Zutritt und Zugang sind mit dem Mitarbeiter vorher terminlich abzustimmen.
- Der Mitarbeiter sichert zu, dass auch die mit ihm in häuslicher Gemeinschaft lebenden Personen mit dieser Regelung einverstanden sind.
- Sollte eine Durchsuchung der Räumlichkeiten, in denen sich das Home-Office befindet, von den Behörden gerichtlich angeordnet werden und steht die Durchsuchung nicht im Zusammen-hang mit der Arbeit des Mitarbeiters bei [Organisationsname], so ist der Zugang zum Home-Office nur nach Rücksprache mit [Organisationsname] zu gewähren. Der Mitarbeit hat in diesem Fall unverzüglich [Organisationsname] über die Durchsuchung zu informieren.

3.4 Anbindung an das Unternehmensnetzwerk

Home-Offices werden ausschließlich durch folgende Lösungen mit dem Unternehmen verbunden

- VPN-Portal: https://sslvpn.[Organisationsname].org
- Citrix-Umgebung: https://citrix.[Organisationsname].org

3.5 Schutz von Informationen

- Der Mitarbeiter hat über alle betrieblichen und geschäftlichen Daten, über die er im Rahmen seiner Tätigkeit, Kenntnis erlangt Stillschweigen zu bewahren. Insbesondere sind betriebliche Unterlagen vor dem Zugriff von Familienmitgliedern und Besuchern zu schützen.
- Die betrieblichen und gesetzlichen Regelungen des Datenschutzes und der Informationssicherheit sind zu beachten und anzuwenden. Daten, Informationen, Passwörter sind vom Mitarbeiter so zu schützen, dass Dritte - insbesondere auch im Haushalt des Mitarbeiters lebende Personen - keine Einsicht und/oder keinen Zugriff nehmen können. Auch beim kurzzeitigen Verlassen des Arbeitsplatzes ist der Bildschirm sofort gemäß der bei [Organisationsname] üblichen Benutzerrichtlinie zu sperren.
- Beim Verlassen des Arbeitsplatzes, welches eine unmittelbare Unterbrechung der Arbeit zur Folge hat, sind alle betriebliche Unterlagen wegzuräumen und verschlossen aufzubewahren.
- Für von [Organisationsname] verwaltete Endgeräte gilt: Die von [Organisationsname] gestellten EDV-Einrichtungen dürfen nicht verändert werden. Dies gilt insbesondere für Änderungen an Hard- und Software. Softwareinstallationen, Softwareanpassungen und Softwaredeinstallationen dürfen nur von Personen durchgeführt werden, die von [Organisationsname] dazu berechtigt und beauftragt wurden.
- Die korrekte Funktion von Schutzeinrichtungen (z. B. Virenscanner) sind möglichst täglich, jedoch immer vor Arbeitsbeginn, gemäß der Anweisungen durch den Mitarbeiter zu überprüfen. Bei einer Fehlermeldung bzw. bei Auffälligkeiten ist unverzüglich der Servicedesk zu verständigen.
- Daten (dies betrifft insbesondere betriebliche Daten) dürfen nur auf fest eingebauten Festplatten der verwalteten Geräte gespeichert werden. Die Nutzung von lokalen externen Festplatten ist untersagt.
- Vorkommnisse, die darauf schließen lassen, dass Endgeräte oder sonstige Gerätschaften nicht ordnungsgemäß funktionieren, sowie Meldungen von Virenscannern, sind dem [Organisationsname] Servicedesk unverzüglich zu melden.
- Die Benutzeranmeldung darf nur über ein Benutzerkonto erfolgen, das über keine lokalen Administratorrechte auf dem Endgerät verfügt.

3.6 Haftung

- Der Mitarbeiter und sonstige in seinem Haushalt lebende Personen haften für Schäden an allen vom Arbeitgeber zur Verfügung gestellten Arbeitsmitteln und Installationen nur bei Vorsatz und grober Fahrlässigkeit.
- Der Mitarbeiter hat Beschädigungen, Verlust oder sonstige Funktionsbeeinträchtigungen der Arbeitsmittel unverzüglich dem Arbeitgeber anzuzeigen und das weitere Vorgehen mit ihm abzustimmen.
- Führt die Störung dazu, dass die Arbeitsleistung nicht an dem häuslichen Arbeitsplatz er-bracht werden kann, muss die Arbeitsleistung auf Verlangen der [Organisationsname] an dem betrieblichen Arbeitsplatz erbracht werden soweit dies dem Mitarbeiter zumutbar ist.

3.7 Aufgabe des Home-Office

- Die Vereinbarung über das Home-Office endet automatisch bei Beendigung des Arbeitsverhältnisses, bei Aufgabe oder Kündigung der Wohnung, in der sich das Home-Office befindet, sowie bei einem Stellenwechsel des Mitarbeiters innerhalb des Betriebs/Unternehmens.
- Die Aufgabe/Kündigung der Wohnung, in der sich das Home-Office befindet, hat der Mitarbeiter der [Organisationsname] unverzüglich anzuzeigen. Nach einem Wohnungswechsel kann eine erneute Einrichtung eines Home-Office erfolgen.
- Die überlassenen Arbeitsmittel sowie alle im Zusammenhang mit dem Home-Office ausgehändigten Unterlagen sind nach Beendigung der Arbeit unverzüglich an die [Organisationsname] zurück zu geben. Dies gilt auch auf Verlangen der [Organisationsname] bei einer längeren Freistellung. Die mit der Rückgabe der Arbeitsmittel entstehenden Kosten trägt [Organisationsname].
- Der Mitarbeiter ist verpflichtet, nach Aufgabe der Arbeit im Home-Office seine gesamte Arbeitsleistung an der betrieblichen Arbeitsstätte zu erbringen, soweit nicht das Arbeitsverhältnis insgesamt beendet wird. Der Mitarbeiter hat während der Arbeit im Home-Office keinen Anspruch auf den vor Beginn innegehabten Arbeitsplatz.