IT SECURITY RICHTLINIE

Dokumenteninformation

Dokumententitel	IT Security Richtlinie
Pfad im OHB	4 Steuerung 4.6 IT&EDV Services 4.6.1 IT Strukturen und Security 4.6.1 IT_Security_Richtlinie_v01
Version	1.0
Geltungsbereich	Alle Mitarbeiter Konzern
Gültig ab	05.02.2019
Gültig bis	31.12.2099
Autor	Barbara Reithofer
Erstellt am	01.02.2019
Redakteur	Paul Gessl
Geprüft und freigegeben am	05.02.2019
GF-genehmigungspflichtig	ja
Genehmigt von GF	Paul Gessl
Genehmigt am	05.02.2019
Publiziert von Redakteur am	06.02.2019
Status	publiziert
Änderungsgrund	Ersterstellung
Dateiname und Pfad	N: Organisationshandbuch/4 Steuerung/ 4.6. IT&EDV Services/4.6.1 IT Strukturen und Security/461_IT_Security_Richtlinie_v01.docx

Dokumentenhistorie

Datum	Version	Änderungsgrund
11.01.2019	1.0	Ersterstellung
05.02.2019	1.1	Ergänzung

Inhaltsverzeichnis

Seite

1. NÖKU IT & EDV Services

Die IT&EDV Services der NÖKU sorgen für die Sicherheit, Wartung und Reparatur, für die Speicherung der anfallenden digitalen Daten, deren tägliche Sicherung und Archivierung sowie für die ausfallsichere Auslegung der informationstechnischen Komponenten.

Datensicherheit (Datenschutz) im Allgemeinen und speziell IT-Sicherheit (Schutz der Systeme) sind unverzichtbar für den Unternehmenserfolg. Unternehmensdaten müssen bestmöglich geschützt werden. Dies gilt sowohl für den Versuch, diese Daten auszuspionieren, als auch für die Gefahr des Datenverlustes durch technische Gebrechen. Durch Computerviren, Spionage und Sabotage sind diese Einrichtungen besonders gefährdet. Unsachgemäße Nutzung, bewusster und unbewusster Missbrauch der informationstechnischen Einrichtungen erhöhen nicht nur das Gefährdungspotential. Sie verursachen auch erhebliche Mehrkosten für Wartung und Reparatur, für die Speicherung der anfallenden digitalen Daten, deren tägliche Sicherung und Archivierung und für die ausfallsichere Auslegung der informationstechnischen Komponenten. Um Sicherheit und Schutz der informationstechnischen Einrichtungen und der gespeicherten Daten zu gewährleisten und die Kosten der Informationstechnologie in akzeptablen Grenzen zu halten, ist es notwendig, dass alle Mitarbeiterinnen und Mitarbeiter unseres Unternehmens mit den informationstechnischen Einrichtungen verantwortungsbewusst und kostenbewusst umgehen.

Ein Verdacht auf Virengefahr, Störungen, Defekte, fehlerhafte Rechtevergabe und auftretende Fehler in Datenanwendungen sind unverzüglich per E-Mail/Ticket an support@noeku.at zu melden.

Die nachfolgend aufgeführten Regelungen der IT Policy werden über diverse Kanäle an die Mitarbeiterinnen und Mitarbeiter kommuniziert (Newsletter, NÖKU News, on Boarding Mappen) und sind von allen Mitarbeiterinnen und Mitarbeiter für einen ordnungsgemäßen Betrieb strikt einzuhalten.

2. IT Sicherheit

2.1 Clear Desk Policy

Unter der Clear Desk Policy versteht man, dass Mitarbeiterinnen und Mitarbeiter alle vertraulichen Dokumente, die sich auf ihrem Arbeitsplatz befinden, verschließen. Unberechtigte Personen (Reinigungspersonal, unbefugte Kolleginnen und Kollegen, oder Besucher) dürfen keinen Zugriff darauf erhalten.

Bitte beachten sie folgende Punkte:

- Bei Verlassen des Arbeitsplatzes müssen alle Ausdrucke, Kopien oder dergleichen mit vertraulichem Inhalt so verstaut werden, dass diese Dokumente nicht für Dritte zugänglich sind (versperrbare Schreibtisch Laden und Kästen, Datenträgersafe).

- Lassen sie keine Ausdrucke im Drucker/Kopierer liegen.
- Verwenden sie immer den „vertraulichen Druck“.
- Bewahren sie unter keinen Umständen Passwortnotizen an Ihrem Arbeitsplatz auf.
- Sperren sie Ihren Computer, wenn sie Ihren Arbeitsplatz verlassen (z. B. unter Windows mit „Windows-Taste + L“)! Unbeaufsichtigte, nicht gesperrte Computer sind ein hohes Sicherheitsrisiko. Unbefugte könnten so Zugang zu vertraulichen Daten erhalten.

2.2 Datenspeicherung

Es stehen allen Mitarbeiterinnen und Mitarbeitern die Datenlaufwerke N:/ und M:/ zur Verfügung.

Alle betrieblichen Daten müssen auf diesen Laufwerken gespeichert werden. Auf dem Laufwerk N:/ steht für jeden Betrieb ein Hauptordner zur Verfügung. Die darunterliegende Datenstruktur und Berechtigungsvergabe wird vom Betrieb bestimmt und verwaltet. Hier erfolgt ein gemeinschaftlicher Zugriff auf die Daten.

Das Laufwerk M:/ ist ihr persönliches Benutzerlaufwerk für betriebliche Zwecke. Auf dieses Laufwerk haben nur sie Zugriff. Das Ablegen privater Daten (Fotos, Musik, etc.) ist nicht gestattet.

Gehen sie mit dem ihnen zur Verfügung gestellten Speicherplatz sorgsam um. Beide Laufwerke werden regelmäßig gesichert. Es ist daher nicht nötig, Daten als Duplikat auf beiden Laufwerken zu speichern.

Bitte beachten sie folgende Punkte:

- Nicht mehr benötigte Dateien sind regelmäßig zu löschen. Damit tragen sie dazu bei, dass die Datenbestände und deren Strukturen überschaubar bleiben und die Kosten der Datenhaltung und Datensicherung in vertretbaren Grenzen bleiben.
- Achten sie bei der Vergabe von Ordner- und Dateinamen auf die Länge und verwenden sie möglichst kurze Begriffe. Die Wiederherstellung eines unbeabsichtigt gelöschten Verzeichnisses ist nur möglich wenn der gesamte Verzeichnispfad (z.B. N:\Betrieb\Ordner\Unterordner\Unterunterordner\Datei.xxx) die Gesamtlänge von max. 200 Zeichen nicht überschreitet. Auch der Aufruf von in so langen Verzeichnisstrukturen abgelegten Dateien aus Anwendungen oder die Anzeige im Explorer kann problematisch sein.
- Zum Datenaustausch mit Partner-Betrieben ist die Business-Dropbox zu verwenden. Unter keinen Umständen dürften betriebliche Daten über private Clouddienste weitergegeben werden.

2.3 Citrix Terminal Server (Citrix Desktop)

Im Citrix Desktop werden alle zentralen Softwareanwendungen der NÖKU für alle Mitarbeiterinnen und Mitarbeiter zur Verfügung gestellt. Die Verwendung des Citrix Desktop bringt eine Reihe von Vorteilen:

Bei Ausfall, Diebstahl oder Virenbefall des lokalen Endgeräts (Client) gehen die auf dem Server gespeicherten Daten nicht verloren, bzw. fallen nicht in unbefugte Hände. Die Software-Anwendungen müssen nur einmal auf dem Terminalserver installiert und gepflegt werden. Der Citrix Desktop bietet zentrale Administration und ein einfach zu steuerndes Sicherheitskonzept, die Daten verlassen die Serverumgebung nicht. Die Leitungskapazität wird geschont, da die Verarbeitung auf den dafür ausgelegten zentralen Servern erfolgt. Die Arbeitsumgebung im Citrix Desktop und über NÖKU Homeoffice (https:\\homeoffice.noeku.at) ist ident.

Bitte beachten sie folgende Punkte:

- Am Citrix Desktop sind die Daten immer in den Netzwerklaufwerken (M:\ oder N:\) abzulegen.
- Die Speicherung von Daten auf lokalen Speicherorten wie Desktop oder Download Ordner ist zu vermeiden bzw. nach Abschluss des Downloads zu bereinigen.
- Dies ist erforderlich, da das lokale Speichern zu erhöhten Anmeldezeiten führt. Bei Anmeldeproblemen werden diese Daten ohne Rückfrage automatisiert bereinigt.
- Beenden Sie eine Terminalserver-Session bitte immer über "Start" / "Abmelden" und nicht durch einfaches Schließen des Fensters. Andernfalls wird Ihre Session zwar geschlossen, läuft aber im Hintergrund am Terminalserver weiter.

2.4 Passwörter und W-LAN Schlüssel

Stellen Sie sich ein Passwort oder einen W-LAN Schlüssel wie einen Schlüssel zu ihrer Wohnung oder zu ihrem Haus vor. Zuhause möchten sie auch ein gutes Schloss besitzen, welches vor einem unbefugten Zutritt schützt. Genauso verhalten sich auch Passwörter. Passwörter schützen vor einem unbefugten Zugang.

Bitte beachten sie folgende Punkte:

- Verwenden sie nie das gleiche Passwort für unterschiedliche Zugänge.
- Verwenden sie Kennwörter, die mindestens 8 Zeichen haben. Ein Passwort muss aus einem Großbuchstaben, Kleinbuchstaben, Ziffern und einem Sonderzeichen bestehen.
- Trivial-Passwörter (hallohallo, abcdefgh, 08/15, 1234 etc.) sind ebenfalls ungeeignet. Sie können von anderen leicht beim Beobachten der Passworteingabe erkannt werden.

- Geben sie ihr Passwort niemanden weiter! Auch Kollegen oder IT-Betreuung benötigen ihr Kennwort nicht.
- Sie müssen Ihr Kennwort alle 3 Monate ändern, es läuft nach 3 Monaten automatisch ab.
- Überlegen sie sich einen Satz und verwenden sie nur die Anfangsbuchstaben für ihr Passwort z.B:
  - „Die Arbeit beginnt jeden Tag um 7 Uhr“ → DAbjTu7U
  - „Samstag arbeite ich von 9 bis 13 Uhr“ → ASaiv9-13U
  - „Am 26. 10. ist Nationalfeiertag“ → a26.10.=N
- Sie sind für ihr Kennwort verantwortlich! Sollten sie den Verdacht haben, dass ein Dritter ihr Kennwort kennt, ändern sie dieses sofort.

2.5 W-LAN Schlüssel

Es stehen an allen NÖKU Standorten mehrere W-LAN Netze zur Verfügung (Büro-, Mobile- und Gast-W-LAN). Diese Netze sind zur internen Verwendung bestimmt. Im Büro W-LAN stehen alle Funktionen zur Verfügung und damit vollständiger Zugriff auf das gesamte Netzwerk der NÖKU Gruppe. Daher ist hier besonders auf Geheimhaltung und Schutz des Zugriffs zu achten. Für Kunden und Besucher der Veranstaltungsorte steht in fast allen Häusern zusätzlich auch noch ein Public W-LAN zur Verfügung, das außerhalb des NÖKU Netzwerkes liegt und auch nicht von den IT&EDV Services der NÖKU verwaltet wird.

Bitte beachten sie folgende Punkte:

- Der Büro W-LAN Schlüssel ist unter allen Umständen geheim zu halten und darf niemals an außenstehende Personen weitergeben werden.
- Das Gast W-LAN darf Außenstehenden für Präsentationen oder temporären Internetzugriff zur Verfügung gestellt werden
- Das Mobile W-LAN ist auf allen Firmenhandys hinterlegt und wird von diesen zwingend automatisch verwendet werden.

2.6 Social Engineering

Unter Social Engineering versteht man das Manipulieren von Personen, um unbefugt Zugang zu vertraulichen Informationen oder IT-Systemen zu erhalten. Vorwiegend wird dieser Angriff per Telefon oder E-Mail durchgeführt.

Social Engineers geben sich gerne als Mitarbeiterinnen oder Mitarbeiter aus. Vielleicht behaupten sie auch, eine Behörde oder ein wichtiges Kundenunternehmen zu vertreten oder zu IT-Abteilung der NÖKU zu gehören. Ihre Opfer werden durch firmeninternes Wissen oder Kenntnisse spezieller Fachbegriffe getäuscht, die sie sich zuvor durch Telefonate oder Gespräche mit anderen Kollegen erworben haben. Beim Angriff appellieren sie dann als „gestresster Kollege“ an Ihre Hilfsbereitschaft oder drohen als „Kunde“ mit dem Verlust eines Auftrages. Kommt ein Social Engineer bei einer Mitarbeiterin oder einem Mitarbeiter nicht ans Ziel, wird der Angriff bei der nächsten Ansprechperson wiederholt – bis er möglicherweise erfolgreich ist.

Bitte beachten sie folgende Punkte:

- Seien sie bei Telefonanrufen oder E-Mails skeptisch, speziell wenn der Wunsch oder der Auftrag der Kollegin oder des Kollegen außergewöhnlich ist.
- Falls möglich, besprechen sie die Angelegenheit mit ihrem Kollegen oder mit ihrer Kollegin persönlich.
- Fragen sie bei verdächtigen E-Mails ihre IT-Abteilung.
- Bedenken sie, dass Social Engineering sehr oft angewandt wird, aber meistens lange Zeit unentdeckt bleibt.
- Geben sie keine vertraulichen Informationen an unbekannte Personen per Telefon oder E-Mail weiter

2.7 Installation von Applikationen

Die selbständige Installation von Applikationen ist untersagt. Dies gilt für alle Arbeits Geräte (PC’s, Notebooks, Server, Tablets) Falls sie eine Applikation benötigen, senden sie eine schriftliche Anfrage an ihre IT Abteilung. Auch harmlos wirkende Applikationen können Schadsoftware enthalten, oder sind Lizenzrechtlich nicht für den Firmeneinsatz freigeben.

2.8 Dokumente richtig entsorgen

Sorglos weggeworfene Dokumente mit vertraulichem Inhalt stellen ein ernstes Sicherheitsproblem dar, wenn diese Daten in falsche Hände geraten. Aus diesem Grund müssen Papier-Dokumente, mit vertraulichem oder Datenschutzrelevantem Inhalt sicher entsorgt werden. Für die sichere Entsorgung eignet sich ein Dokumenten-Schredder den ein Dienstleistungsunternehmen, welches sich auf die sichere Entsorgung spezialisiert hat, fachgerecht entsorgt.

Bitte beachten sie folgende Punkte:

- Werfen sie vertrauliche Dokumente auf keinen Fall in den Papierkorb! Sofern es sich um Inhalte handelt, die Außenstehenden nicht zugänglich gemacht werden dürfen, müssen die Dokumente sicher entsorgt werden. Beachten sie, dass diese Vorgehensweise auch bei Archivmaterial einzuhalten ist.

2.9 Backup der Daten

Es werden generell nur Daten der Laufwerke M:\ und N:\ sowie Daten der von der NÖKU IT zentral zur Verfügung gestellten Datenanwendungen gesichert. Daten die auf lokalen Datenträgern (zB Laufwerk C:\) bzw. nicht eingebundenen externen Speichermedien abgelegt werden, sind nicht im Backup enthalten. Das Speichern von betrieblichen Daten auf lokalen Datenträgern und nicht eingebundenen externen Speichermedien ist daher untersagt.

2.10 Umgang mit mobilen IT-Geräten

Mobile IT Geräte (Notebooks, Tabletts, Wechselmedien...) stellen durch ihre mobile Verwendung ein erhöhtes Sicherheitsrisiko dar. Portable Geräte sind für Diebe ein attraktives Ziel.

Unternehmensinterne Daten dürfen nur mit Genehmigung der Geschäftsleitung das Firmengelände verlassen oder außerhalb des Firmengeländes verwendet werden. Daher ist insbesondere bei mobilen IT Geräten darauf zu achten, dass keine beruflichen Daten direkt auf der Festplatte des Geräts gespeichert werden.

Bitte beachten sie folgende Punkte:

- Lassen sie das Gerät nicht unbeaufsichtigt.
- Überlassen sie das Gerät nicht anderen Personen.
- Achten sie bei Passworteingabe am Gerät auf ihren Sichtschutz – ähnlich wie bei einem Bankomaten.
- Verwenden sie ihren privaten Cloud-Speicher nicht für Unternehmensdaten.
- Melden sie einen Diebstahl oder Verlust sofort der IT-Abteilung.
- Bei Verwendung der betriebsinternen Anwendungen Webmail und Citrix Receiver (https:\\homeoffice.noeku.at) achten Sie auf ein korrektes Abmelden der Sitzung damit kein unbefugter Zugriff auf die Firmenstrukturen erfolgen kann.

2.11 Wechselmedien

Als Wechselmedien gelten alle externen Datenträger wie z.B. USB-Sticks, SD Karten, externe Festplatten, CD's, DVD's, Smartphones die per USB angeschlossen werden…. Der Einsatz stellt ein großes Sicherheitsrisiko dar. Speziell wenn diese Datenträger von externen Quellen stammen. Auf diesen Wechselmedien kann sich Schadsoftware verstecken, welche das gesamte Firmennetzwerk lahmlegen kann.

Bitte beachten sie folgende Punkte:

- Verwenden sie niemals Wechselmedien aus unbekannter Herkunft
- Verwenden sie nach Möglichkeit neue bisher unbenutzte Medien, im Zweifelsfall bitte im IT Service Center prüfen und neu formatieren lassen
- Wechselmedien mit äußerster Sorgfalt behandeln und verwahren
- Inhalte nach Möglichkeit am externen Datenträger mit Passwortschutz absichern.
- Übergeben sie die nicht mehr benötigten Datenträger Ihrer IT-Abteilung bzw. einer eigens zu diesem Zweck bestimmten Person, die für die sichere Entsorgung zuständig ist.

2.12 Firmenhandynutzung

Smartphones stellen erhöhtes Sicherheitsrisiko bezüglich Diebstahls, Verlusts und betriebssystemtechnischen Schwachstellen dar, daher ist darauf zu achten dass berufliche Daten nur innerhalb des geschützten Containers auf dem Gerät gespeichert und verarbeitet werden.

Es steht jeder/m Mitarbeiterinnen und Mitarbeiter das Tarifpaket - A1 Mobile Enterprise Europe Medium Paket(3000 min. in alle Netze United Europa Area und Datenpaket 7 GB) zur Verfügung

Für seitens der Geschäftsführung genehmigte Dienstreisen in Länder, die nicht im Tarifpaket enthalten sind, können Zusatzpakete aktiviert werden. Bezüglich der Telefonkostenabrechnung wird für jede Teilnehmernummer ein monatlicher Einzelgesprächsnachweis geführt und protokolliert.

Bitte beachten sie folgende Punkte:

- Sowohl die SIM-Karte insbesondere jedoch das Handy-Gerät sind sorgsam zu benutzen und müssen bei der Rückgabe voll funktionstüchtig sein.
- Verwenden Sie das Gerät nicht ohne Glasschutz-Folie und Hülle.
- Lassen Sie das Gerät nicht unbeaufsichtigt.
- Überlassen Sie das Gerät nicht anderen Personen.
- Achten Sie bei der Passworteingabe am Gerät auf ihren Sichtschutz – ähnlich wie bei einem Bankomaten.
- Sie können zur einfacheren Bedienung die Fingerprintfunktion auf dem Gerät einrichten. Diese biometrischen Daten stellen sensible Daten im Sinne des Datenschutzes dar und sind damit auf dem Handy gespeichert, sie werden nicht auf einen zentralen Server übertragen.
- Verändern Sie keine Einstellungen die bei der Übergabe des Geräts vordefiniert wurden.
- Melden Sie einen Diebstahl oder Verlust sofort der IT-Abteilung.
- Durch den Einsatz des gesicherten Containers steht das Gerät unter Fernwartung. Im Falle von Diebstahl oder Verlust /Defekt wird das Handy und alle Daten die sich darauf befinden gelöscht. Daten die außerhalb des Containers auf dem Gerät sind, werden als private Daten gesehen und daher nicht gesichert, sorgen Sie für eine regelmäßige Sicherung dieser Daten(Bilder, etc.) und speichern Sie keine geschäftlichen Kontakte und Daten auf dem Gerät. Insbesondere wenn eine Reparatur des Gerätes nötig ist, werden alle Daten gelöscht und das Gerät auf Werkseinstellungen zurückgesetzt.
- Achten Sie auf eventuelle Daten- und Gesprächspaketvolumen um zusätzliche Kosten für das Unternehmen zu vermeiden.
- Personenbezogene Daten (Kontakte) die Sie beruflich benötigen, dürfen nicht auf dem Handy selbst gespeichert werden, diese sind in der gesicherten Container-App bzw. über Outlook zu speichern und zu verwalten.
- Verwenden Sie ihren privaten Cloud-Speicher oder andere Apps nicht für Unternehmensdaten.
- Sie können auf dem Gerät Apps installieren, z. B. WhatsApp, Wetter-App, ÖBB Fahrplan, etc. Diese dürfen ausschließlich privat genutzt werden, es dürfen keine personenbezogenen Daten aus dem beruflichen Umfeld kommuniziert werden und es dürfen keine zusätzlichen Kosten für das Unternehmen entstehen. (Daten- u. Gesprächspaketvolumen, kostenpflichtige Abos oder Apps)

2.13 E-Mail Nutzung

E-Mail gehört zur Standardausrüstung eines Arbeitsplatzes. Dadurch lohnt es sich auch für Kriminelle diese Form der Kommunikation zu nutzen. Somit landen aber auch Spam-, Hoax- oder Phishing-Mails sowie mit Schadprogrammen verseuchte Nachrichten in ihrem Posteingang. Solche unerwünschten Nachrichten – mit mehr oder weniger gefährlichem Inhalt – machen ca. zwei Drittel des gesamten NÖKU E-Mail-Aufkommens aus. Von etwa 300.000 einlangenden monatlichen E-Mails werden rund 210.000 durch die SPAM-Firewall geblockt.

Bitte beachten sie folgende Punkte:

- Öffnen sie keine E-Mails, wenn ihnen Absender oder Betreffzeile verdächtig erscheinen.
- Öffnen sie niemals Dateianhänge, die ihnen verdächtig vorkommen. Auch bei vermeintlich bekannten und vertrauenswürdigen Absendern ist zu prüfen: Passt der Text der E-Mail zum Absender (englischer Text von deutschsprachigem Absender, unsinniger Text, fehlender Bezug zu aktuellen Vorgängen etc.)? Erwarten sie die beigelegten Dateien, passen sie zum Absender oder kommen diese völlig unerwartet?
- Öffnen sie keine E-Mails mit Spaßprogrammen, da diese oftmals Schadsoftware enthalten.
- Sogenannte Phishing-Mails, die zur Übermittlung von persönlichen Online-Banking-Daten oder Passwörtern (z.B. PIN oder TAN) auffordern, müssen sofort gelöscht werden. Die angeforderten, vertraulichen Informationen dürfen sie auf keinen Fall weitergeben.
- Eine automatisierte Weiterleitung bzw. generell die Weiterleitung beruflicher E-Mails an private Accounts ist untersagt.
- Oftmals kann in einem E-Mail ein Link angeklickt werden, um eine Webseite aufzurufen. Seien sie dabei vorsichtig: In betrügerischen E-Mails wird diesen Links oft eine völlig andere Internet-Adresse hinterlegt, als im Mail zu sehen ist. Beim Anklicken wird dann eine gefälschte Phishing-Webseite aufgerufen oder sogar Schadsoftware installiert. Sicherer ist es, den Link mittels „Hyperlink kopieren“ in den Browser zu übertragen und ihn vor dem Aufrufen noch einmal zu überprüfen.
- Beantworten sie keine Spam-Mails! Die Rückmeldung bestätigt dem Spam-Versender nur die Gültigkeit Ihrer Mail-Adresse und erhöht dadurch Ihr Risiko, weitere Zusendungen zu erhalten. Das Abbestellen von E-Mails ist nur bei seriösen Zustellern sinnvoll.
- Benachrichtigen sie auch Ihre Kolleginnen und Kollegen über verdächtige Zusendungen. Besprechen sie die aktuellen E-Mails, die sie als Phishing-Versuche oder Virus-Mails erkannt haben, um gemeinsam die typischen Kennzeichen kennenzulernen. Sie können auf diese Weise sehr rasch Ihre Erkennungsfähigkeit trainieren und verbessern.
- Fragen sie ihre IT-Abteilungen, falls sie sich unsicher sind.
- Denken sie bei ihrem Urlaubsantritt oder bei Abwesenheit an den Abwesenheitsassistenten, um die Absender über ihre Abwesenheit zu informieren.
- Nicht mehr benötigte Dateien und E-Mails sind regelmäßig zu löschen und damit dazu beizutragen, dass die Datenbestände und deren Strukturen überschaubar

2.14 Nutzung privater IT Geräte (BYOD - Bring your own device)

Die Nutzung und Einbindung privater IT Geräte (Notebooks, Tablets, Handys, private Drucker im mobilen Arbeiten,…) in firmeninterne Strukturen ist untersagt. Es darf keine Verbindung mittels Netzwerkkabel oder Büro W-LAN hergestellt werden. Ein Active Sync mit dem Firmenpostfach darf auf privaten Smartphones oder anderen IT-Geräten nicht eingerichtet werden.

Einzig die Nutzung des Webmail Zugangs und über den Citrix Receiver (https:\\homeoffice.noeku.at) ist mit privaten Geräten möglich und gestattet.

Bitte beachten sie folgende Punkte:

- Lassen sie das Gerät nicht unbeaufsichtigt wenn sie aktive Sitzungen im Citrix Receiver oder im Webmail offen haben
- Überlassen sie das Gerät in diesem Fall nicht anderen Personen.
- Achten sie bei Passworteingabe am Gerät auf ihren Sichtschutz – ähnlich wie bei einem Bankomaten.
- Verwenden sie ihren privaten Cloud-Speicher nicht für Unternehmensdaten.
- Speichern sie unter keinen Umständen firmeninterne Daten auf ihr lokales Laufwerk
- Achten Sie auf ein korrektes Abmelden der Sitzungen, damit kein unbefugter Zugriff auf die Firmenstrukturen erfolgen kann.

2.15 Private Nutzung der NÖKU IT-Infrastruktur

Die informationstechnischen Einrichtungen, besonders E-Mail und der Zugriff auf das Internet, dürfen nur in geringem Ausmaß und in Arbeitspausen privat genutzt werden. Auf den Laufwerken (N:/ und M:/) und lokal auf den Arbeitsgeräten dürfen keine privaten Daten gespeichert werden. Es ist empfohlen private E-Mails sofort zu löschen. Ansonsten sind private E-Mails in einem gekennzeichneten Unterordner des Posteingangs abzulegen, damit diese bei Verlassen des Unternehmens auch von ihnen in einem Vorgang gesichert gelöscht oder übertragen werden können.

2.16 Warnungen und Fehlermeldungen

Warnungen oder Fehlermeldungen die sie nicht selbst verursacht haben, bzw. die sie nicht lösen können, müssen unverzüglich der IT Abteilung gemeldet werden. (E-Mail an support@noeku.at)