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_v02
Version	1.2
Geltungsbereich	Alle Mitarbeiter Konzern
Gültig ab	10.11.2020
Gültig bis	31.12.2099
Autor	Barbara Reithofer
Erstellt am	01.11.2020
Redakteur	Paul Gessl
Geprüft und freigegeben am	10.11.2020
GF-genehmigungspflichtig	ja
Genehmigt von GF	Paul Gessl
Genehmigt am	10.11.2020
Publiziert von Redakteur am	10.11.2020
Status	publiziert
Änderungsgrund	Ergänzungen
Dateiname und Pfad	N: Organisationshandbuch/4 Steuerung/ 4.6. IT&EDV Services/4.6.1 IT Strukturen und Security/461_IT_Security_Richtlinie_v2.docx

Dokumentenhistorie

Datum	Version	Änderungsgrund
11.01.2019	1.0	Ersterstellung
05.02.2019	1.1	Ergänzung
10.11.2020	1.2	Ergänzung

Inhaltsverzeichnis

Seite

1. NÖKU IT & EDV Services 5
2. IT Sicherheit 6
2.1 NOEKU Desktop (Citrix Workspace App) 6
2.2 Mobiles Arbeiten 7
2.3 Microsoft TEAMS 7
2.4 Clear Desk Policy 8
2.5 Datenspeicherung 8
2.6 Festlegen von Passwörtern 9
2.7 W-LAN Nutzung und Verfügbarkeit 10
2.8 Awareness 11
2.9 Installation von Applikationen 12
2.10 Datenträger und USB-Sticks 12
2.11 Firmenhandynutzung 13
2.12 E-Mail Nutzung 14
2.13 Informationsklassifizierung 15
2.14 Makros 17
2.15 Nutzung privater IT Geräte (BYOD - Bring your own device) 17
2.16 Private Nutzung der NÖKU IT-Infrastruktur 18

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 Mitarbeitern für einen ordnungsgemäßen Betrieb strikt einzuhalten. Weiterführende Informationen und Anleitungen finden sie unter status.noeku.at

2. IT Sicherheit

2.1 NOEKU Desktop (Citrix Workspace App)

Für den Zugriff auf alle zentralen Softwareanwendungen der NÖKU-Gruppe steht der NOEKU Desktop allen Mitarbeitenden zur Verfügung und ist und ist zwingend als zentraler, digitaler Arbeitsplatz zu verwenden. Lokales Arbeiten auf PC´s und Laptopts ist, bis auf die definierten Ausnahmen (Kassenarbeitsplätze/ technische Programme und Zugriffe) unbedingt zu vermeiden.

Die Verwendung des NOEKU Desktop bringt eine Reihe von Vorteilen:

- Bei Ausfall, Diebstahl oder Virenbefall des lokalen Endgeräts gehen die auf dem Server gespeicherten Daten nicht verloren, bzw. fallen nicht in unbefugte Hände.
- Die Software-Anwendungen werden zentral gewartet und mit den passenden Lizenzen versehen.
- Der Citrix Desktop bietet zentrale Administration und ein einfach zu steuerndes Sicherheitskonzept, die Daten verlassen die Serverumgebung nicht.
- Die Leitungskapazität an ihrem Arbeitsplatz wird geschont, da die Verarbeitung aller Daten auf den dafür ausgelegten zentralen Servern erfolgt. Die Arbeitslast liegt daher auf den zur Verfügung stehenden Servern und es erfolgt nur eine Übertragung (Streaming) ihres Desktops auf das verwendete Arbeitsgerät.
- Die Arbeitsumgebung im Citrix Desktop und über NÖKU Mobiles Arbeiten (https:\\noeku.cloud.com) ist ident.

Bitte beachten sie folgende Punkte:

- Legen Sie am Citrix Desktop die Daten immer in den Netzwerklaufwerken („Dokumente“ oder N:\) ab.
- Speichern Sie keine Daten auf lokalen Speicherorten, wie Desktop oder Download-Ordner. 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.

2.2 Mobiles Arbeiten

Der Fernzugriff auf das Unternehmensnetzwerk der NÖKU-Gruppe erfolgt über einen Browseraufruf – noeku.cloud.com – bzw. bei IGEL Geräten über den Login Button links oben. Nach der erfolgten 2 Faktor Authentifizierung mittels MS Authenticator erfolgt der Einstieg in den NÖKU Desktop über die am Gerät zu installierende Citrix Workspace App.

Dieser Zugriff ist sowohl mit Firmengeräten als auch mit privaten Geräten von überall her möglich und erlaubt. Der NÖKU Desktop ist im Funktionsumfang völlig ident mit dem innerhalb der Betriebe angebotenen Arbeitsumgebung. Die Daten verlassen dabei die gesicherte Systemumgebung nicht und können auch nicht aus dem NÖKU Desktop auf die lokalen Speicher gelegt werden bzw. von dort bezogen werden. Somit sind potenzielle Schäden, wie der Verlust sensibler oder vertraulicher Daten, Imageverlust, Schäden an kritischen Systemen oder Geldbußen in großem Maß ausgeschlossen.

2.3 Microsoft TEAMS

Microsoft TEAMS ermöglicht übergreifende moderne Kommunikation und Zusammenarbeit. Ziel ist es, interne Abläufe effizienter zu gestalten, Wissensaustausch zu steigern und Abstimmungen zu vereinfachen. TEAMS ermöglicht gemeinsames arbeiten an Dokumenten und das Bereitstellen und Austauschen von Informationen. In agilen Gruppen können sich MitarbeiterInnen digital und selbständig organisieren, kommunizieren und zusammenarbeiten.

Bitte beachten sie folgende Punkte:

- Orientieren und halten Sie sich an den gemeinsamen „Spielregeln“. Informationen dazu finden Sie unter „http://status.noeku.at/display/help/MS+Teams“.
- Informieren Sie sich über Ihren Team-Besitzer. Der Team-Besitzer ist innerhalb von TEAMS der Informationsmanager und Kommunikationsmanager.
- Der Team-Besitzer ist zuständig und verantwortlich für die Schulung der Team-Member.
- Achten Sie bei der Datenübermittlung zu Externen oder Gästen auf die Vertraulichkeit der Dokumente.
- Vermeiden Sie Duplikate von Dokumenten. Zum Beispiel senden Sie dieselben Dokumente nicht per E-Mail und über TEAMS.

2.4 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, unbefugten Kolleginnen und Kollegen, oder Besucher) dürfen keinen Zugriff darauf erhalten.

Bitte beachten sie folgende Punkte:

- Bewahren Sie Passwortnotizen nicht am Arbeitsplatz oder einem anderen zugänglichen Ort auf.
- Sperren Sie beim Verlassen des Arbeitsplatzes den Computerbildschirm (z.B. unter Windows mit „Windows-Taste + L“).
- Schalten Sie am Ende jedes Arbeitstages den Computer vollständig ab
- Wenn Sie Laptops oder Tablets nicht benutzen, sichern Sie diese mit einem Laptopschloss oder sperren sie in einer Schublade ein.
- Trennen Sie alle Hardware-Token, Smartcards, USB-Token usw. von Ihrem Computer, wenn Sie diese nicht verwenden.
- Bewahren Sie Massenspeichergeräte, wie beispielsweise USB-Sticks, bei Nichtgebrauch in einer verschlossenen Schublade auf.
- Entfernen Sie am Ende jedes Arbeitstages alle vertraulichen oder streng vertraulichen Informationen vom Schreibtisch und verstauen diese so, dass sie für andere nicht zugänglich sind.
- Entfernen Sie Ausdrucke mit vertraulichen oder streng vertraulichen Informationen sofort aus dem Drucker.
- Löschen Sie Whiteboards mit vertraulichen oder streng vertraulichen Informationen beim Verlassen des Raumes.
- Entsorgen Sie vertrauliche oder streng vertrauliche Dokumente in die dafür vorgesehenen Behälter, auf keinen Fall in einem Papierkorb.
- Bewahren Sie Schlüssel die für den Zugriff auf vertrauliche oder streng vertrauliche Informationen dienen, nicht an einem unbeaufsichtigten Schreibtisch auf.

2.5 Datenspeicherung

Es stehen allen Mitarbeitenden der NÖKU-Gruppe die Datenlaufwerke „Dokumente“ und N:\ sowie OneDrive zur Verfügung, welche regelmäßig gesichert werden. Es ist nicht nötig und erwünscht, Daten als Duplikat auf mehreren Laufwerken zu speichern.

- 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.

- „Dokumente“ ist Ihr persönliches Benutzerlaufwerk für betriebliche Zwecke. Auf dieses Laufwerk haben nur Sie Zugriff. Das Ablegen privater Daten (Fotos, Musik, etc.) ist nicht gestattet.
- „OneDrive“ ist eine Schnittstelle zwischen der Ablage auf N:\ bzw. „Dokumente und den Dateien in MS Teams. Es ermöglicht einen einfachen Transport bzw. auch die Möglichkeit Dateien aus MS Teams lokal über die Ordnerstruktur zu öffnen und zu bearbeiten

Alle Daten der Laufwerke „Dokumente“ und N:\ sowie Daten der von der NÖKU IT-Abteilung zentral zur Verfügung gestellten Datenanwendungen werden regelmäßig gesichert.

Bitte beachten sie folgende Punkte:

- Speichern Sie alle betrieblichen Daten auf den Laufwerken N:\ und „Dokumente“.
- Gehen Sie mit dem zur Verfügung stehenden Speicherplatz sorgsam um und löschen Sie nicht mehr benötigte Dateien regelmäßig, damit die Datenbestände und deren Strukturen überschaubar 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, da die Wiederherstellung eines unbeabsichtigt gelöschten Verzeichnisses nur möglich ist, wenn der gesamte Verzeichnispfad (z.B. N:\Betrieb\Ordner\Unterordner\Unterunterordner\Datei.xxx) die Gesamtlänge von max. 200 Zeichen nicht überschreitet.
- Verwenden Sie zum Datenaustausch mit Partner-Betrieben CELUM.
- Speichern Sie keine betrieblichen Daten auf Wechseldatenträgern, wie z.B. USB-Sticks.
- Geben Sie unter keinen Umständen betriebliche Daten über private Cloud-Dienste weiter.
- Achten Sie bei der Ablage der Daten in MS Teams auf die Vertraulichkeit, vor allem wenn Sie in den Teams mit Externen zusammenarbeiten

2.6 Festlegen von Passwörtern

Passwörter sind ein wichtiger Bestandteil der Informationssicherheit und dienen dem Schutz von Benutzerkonten. Ein schlecht gewähltes Passwort kann jedoch zu unbefugtem Zugriff und/oder unbefugter Nutzung von Ressourcen der NÖKU-Gruppe führen.

Bitte beachten sie folgende Punkte:

- Verwenden Sie unterschiedliche Passwörter für unterschiedliche Systeme.
- Erstellen Sie Passwörter, die 8 Zeichen haben und aus einem Großbuchstaben, Kleinbuchstaben, Ziffern und einem Sonderzeichen bestehen. Eine Möglichkeit wäre, sich einen Satz zu überlegen und davon die Anfangsbuchstaben zu verwenden, z.B.:
  - „Die Arbeit beginnt jeden Tag um 7 Uhr!“ DAbjTu7U!
  - „Am Samstag arbeite ich von 9 bis 13 Uhr.“ ASaiv9-13U.
  - „Am 26. 10. ist Nationalfeiertag!“ a26.10.=N!
- Ändern Sie das Passwort sofort, wenn Sie das Gefühl haben, dass ein Dritter Ihr Passwort kennt.
- Verwenden Sie keine trivialen Passwörter, wie hallohallo, abcdefgh, qwertz, 08/15, 1234 etc. oder Passwörter mit persönlichen Informationen (wie Geburtsdaten, Adressen, Telefonnummer, Namen von Familienmitgliedern, Haustieren oder Freunden), da die Gefahr besteht, von Dritten beim Eingeben des Passworts beobachtet zu werden.
- Geben Sie Passwörter in keinem Fall weiter. Dies inkludiert Kolleginnen, Kollegen oder die IT-Betreuung.

2.7 W-LAN Nutzung und Verfügbarkeit

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.
- Private Mobiltelefone, Notebooks und sonstige private Geräte dürfen in keinem Fall in das Büro-, Mobile-, oder Gast-WLAN der NÖKU-Gruppe eingebunden werden.
- Das zur Verfügung stehende W-LAN darf nicht für private Zwecke, wie z.B. Streaming-Dienste, verwendet werden.

2.8 Awareness

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.

Beispiele für Social Engineering Angriffe sind:

- Ein Unbekannter fordert Sie auf, ein Dokument (wie beispielsweise eine Mahnung, Rechnung oder Bestellbestätigung) zu öffnen.
- Jemand gibt sich per Telefon oder E-Mail als Kunde, Dienstleister oder Bekannter von Ihnen aus, allerdings ist Ihnen die E-Mail Adresse oder die Telefonnummer der Person nicht bekannt.
- Jemand bittet Sie, Geld zu überweisen, eine Kundenkontonummer zu ändern oder Ihre Kontodaten preiszugeben, ohne zuvor mit Ihnen darüber gesprochen zu haben.

Bitte beachten sie folgende Punkte:

- Seien Sie bei Telefonanrufen oder E-Mails skeptisch, speziell wenn der Wunsch oder der Auftrag des Anrufers oder vermeintlichen Kollegin oder Kollege außergewöhnlich sind.
- Besprechen Sie Angelegenheiten, wenn möglich, persönlich mit Kolleginnen und Kollegen.
- Melden Sie verdächtige E-Mails oder Anrufe dem IT-Service Center (support@noeku.at).
- Geben Sie keine vertraulichen Informationen an unbekannte Personen weiter, weder persönlich noch per Telefon oder E-Mail.

2.9 Installation von Applikationen

Die selbständige Anschaffung und Installation von Softwareprodukten, Applikationen oder ähnlichen Produkten ist untersagt. Dies gilt für alle Arbeits Geräte (PC's, Notebooks, Server, Tablets) Falls sie eine Anschaffung planen oder eine zusätzliche Software benötigen, senden sie eine schriftliche Anfrage per E-Mail – softwarewunsch@noeku.at an ihre IT Abteilung. Auch harmlos wirkende Applikationen können Schadsoftware enthalten oder sind Lizenzrechtlich nicht für den Firmeneinsatz freigeben.

2.10 Datenträger und USB-Sticks

Datenträger und USB-Sticks stellen durch ihre mobile Verwendung ein erhöhtes Sicherheitsrisiko dar und sind für Diebe ein attraktives Ziel. Der Schutz der Daten auf diesen Geräten wird durch die Verwendung in verschiedenen Umgebungen, welche nicht immer risikofrei sind, erschwert.

Als Wechselmedien gelten dabei alle externen Datenträger, wie z.B. USB-Sticks, SD Karten, externe Festplatten, CDs, DVDs, Smartphones, die per USB angeschlossen werden. Speziell wenn diese Datenträger von externen Quellen stammen, stellt deren Einsatz ein großes Sicherheitsrisiko dar, da diese Schadsoftware enthalten können, welche das gesamte Firmennetzwerk lahmlegen kann. Daher ist der Zugriff und das Schreiben auf Datenträgern generell untersagt und auch technisch unterbunden. Wo es möglich ist, greifen sie für einen Datenaustausch mit Externen auf Celum oder für gemeinsame Bearbeitung auf

die Möglichkeiten von MS Teams zurück.

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.
- Wenn es für sie unerlässlich ist, Datenträger zu verwenden, wenden sie sich bitte an die IT-Abteilung um die dafür nötige Berechtigung und Hardware zu erhalten

2.11 Firmenhandynutzung

Da Smartphone ein erhöhtes Sicherheitsrisiko bezüglich Diebstahl, Verlust und betriebs-systemtechnischen Schwachstellen darstellen ist darauf zu achten, dass berufliche Daten nur innerhalb des geschützten Containers gespeichert und verarbeitet werden.

Allen Mitarbeitenden steht das Tarifpaket „A1 Mobile Enterprise Europe Medium“ (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, müssen rechtzeitig Zusatzpakete angefordert und aktiviert werden, um zusätzliche Kosten für das Unternehmen zu vermeiden.

Bitte beachten sie folgende Punkte:

- Benützen Sie sowohl die SIM-Karte als auch das Smartphone sorgsam und achten Sie darauf, dass es bei der Rückgabe voll funktionstüchtig ist.
- Schützen Sie das Smartphone mit einem Code oder der Fingerprintfunktion. Biometrische Daten stellen sensible Daten im Sinne des Datenschutzes dar und sind auf dem Handy, nicht auf einem zentralen Server, gespeichert.
- Achten Sie bei der Passworteingabe am Smartphone auf den Sichtschutz (ähnlich wie bei einem Bankomaten).
- Verändern Sie keine Einstellungen, die bei der Übergabe des Smartphones vordefiniert wurden.
- Die Installation von Apps, wie OEBB-Fahrplan, etc., auf dem Smartphone ist erlaubt. Sie dürfen diese Apps jedoch ausschließlich privat nutzen. Die Kommunikation von personenbezogenen Daten aus dem beruflichen Umfeld über diese Apps ist untersagt. Zudem dürfen keine zusätzlichen Kosten für die NÖKU-Gruppe entstehen. (durch Daten- u. Gesprächspaketvolumen, kostenpflichtige Abos).
- Verwenden Sie das Smartphone nicht ohne Displayschutzfolie und Hülle.
- Lassen Sie das Smartphone nicht unbeaufsichtigt.
- Überlassen Sie das Smartphone keinen Dritten.
- Verwenden Sie keinen privaten Cloud-Speicher für Unternehmensdaten.
- Daten, die außerhalb des Containers auf dem Gerät gespeichert sind, werden als private Daten gesehen und daher nicht gesichert. Sorgen Sie aus diesem Grund für eine regelmäßige Sicherung dieser Daten (Bilder, etc.).
- Melden Sie den Diebstahl/Verlust des Smartphones sofort dem IT-Service Center (support@noeku.at).

2.12 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:

- Legen Sie private E-Mails in einem gekennzeichneten Unterordner Ihres Posteinganges ab.
- 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? Erwarten sie die beigelegten Dateien, passen sie zum Absender oder kommen diese völlig unerwartet?
- 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.
- Melden Sie verdächtige E-Mails dem IT-Service Center (support@noeku.at).
- 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.
- Aktivieren Sie vor Urlaubsantritt oder bei längerer Abwesenheit den Abwesenheitsassistenten, um Dritte über Ihre Abwesenheit zu informieren.
- Löschen Sie regelmäßig nicht mehr benötigte E-Mails.
- Öffnen Sie Links in E-Mails mittels „Hyperlink kopieren“, um die Weiterleitung auf sogenannte Phishing-Webseiten verhindern zu können.

2.13 Informationsklassifizierung

In allen Dokumenten der MS Office Anwendungen steht ein vierstufiges Informationsklassifizierungssystem zur Verfügung. Das bedeutet, dass alle Informationen, Daten, Dokumente und Werte gemäß einer der vier Klassen Öffentlich, Intern, Vertraulich oder Streng vertraulich gekennzeichnet werden können. Die Standardeinstellung innerhab der NÖKU Gruppe ist dabei immer „Intern“

Bitte beachten sie folgende Punkte:

- Kennzeichnen Sie Informationen mit der Klasse **Öffentlich**, wenn Sie die folgende Frage bejahen können: *Würden Sie diese Informationen auf einer Website veröffentlichen und an Dritte weitergeben?*
  - In diese Gruppe fallen beispielsweise veröffentlichte Finanzberichte, Pressemitteilungen, Broschüren, wöchentliche Kantinenmenüs, Informationen, die auf der NÖKU-Website veröffentlicht wurden.
  - Sie dürfen Informationen, die mit **Öffentlich** gekennzeichnet sind, innerhalb und außerhalb der NÖKU-Gruppe frei verbreiten.
- Kennzeichnen Sie Informationen mit der Klasse **Intern**, wenn Sie die folgende Frage bejahen können: *Würden Sie diese Informationen an jeden Mitarbeiter innerhalb der NÖKU-Gruppe weitergeben, ohne potenzielle Schäden zu riskieren?*
  - Beispiele dafür sind Richtlinien, Angebote und Mitschriften eines Meetings.
  - Sie dürfen Informationen, die mit **Intern** gekennzeichnet sind, innerhalb der NÖKU-Gruppe frei verbreiten.
  - Werden Informationen nicht gesondert gekennzeichnet, fallen sie automatisch in die Gruppe **Intern**.
- Kennzeichnen Sie Informationen mit der Klasse **Vertraulich**, wenn Sie die folgende Frage bejahen können: *Sind diese Informationen nur für eine begrenzte Gruppe bestimmt und wären weitere Offenlegungen innerhalb oder außerhalb des Unternehmens potenziell schädlich?*
  - Beispiele dafür sind Gehaltslisten und Bonuslisten.
  - Sie dürfen Informationen, die mit **Vertraulich** gekennzeichnet sind, nur an einen begrenzten, definierten Empfängerkreis weitergeben
- Kennzeichnen Sie Informationen mit der Klasse **Streng vertraulich**, wenn Sie die folgende Frage bejahen können: *Wenn Sie diese Informationen an potenzielle Investoren/Kunden weitergeben würden, würden diese daraus einen geschäftsrelevanten Vorteil (z.B. Kauf/Verkauf von Aktien) ziehen?*
  - Beispiele dafür sind Passwörter, Unterlagen der Geschäftsführung und Gesundheitsdaten.
  - Sie dürfen Informationen, die mit **Vertraulich** gekennzeichnet sind, nur an eine begrenzte Gruppe von benannten Personen weitergeben
- Sie dürfen Informationen der Klasse **Intern** nicht an Empfänger außerhalb der NÖKU-Gruppe verteilen.
- Sie dürfen Informationen der Klasse **Vertraulich** oder **Streng vertraulich** nicht an Personen außerhalb des definierten Empfängerkreises weitergeben

2.14 Makros

Makros sind nützliche Hilfsprogramme und Skripte in Office-Dokumenten. Sie werden in Tabellenkalkulationen, in der Textverarbeitung und in Datenbanken eingesetzt. Sie erleichtern und beschleunigen die Arbeit, indem häufig benötigte Befehlsfolgen mit Hilfe eines Makros automatisiert durchgeführt werden. Im Tagesgeschäft sind Makros jedoch eher unüblich und kommen vor allen in PowerPoint Präsentationen oder Word-Dokumenten sehr selten vor.

Da Makros auch von Angreifern verwendet werden können, um Schadsoftware oder Viren in Computer einzuschleusen, ist das Ausführen von Makros in Office-Dokumenten automatisch deaktiviert. Makros in Office-Dokumenten sind eine der Hauptverbreitungsquellen bei Angriffen mit Verschlüsselungstrojanern (Ransomware).

Bitte beachten sie folgende Punkte:

- Aktivieren Sie Makros nur wenn Sie wissen, wofür das Makro notwendig ist.
- Aktivieren Sie Makros nur, wenn Sie die Datei von einer vertrauenswürdigen Person bekommen haben und diese Person Sie darüber informieren kann, ob das Makro sicher ist und wer es erstellt hat.
- Aktivieren Sie Makros niemals, wenn Sie die Datei von einem Unbekannten oder einer nicht vertrauenswürdigen Person erhalten haben.
- Aktivieren Sie Makros niemals, wenn Sie die Daten auf einem fremden USB Stick gefunden oder aus dem Internet heruntergeladen haben.
- Aktivieren Sie das Makro nicht, wenn Sie nicht wissen, wozu das Makro notwendig ist.
- Aktivieren Sie das Makro nicht, wenn Sie beim Öffnen eines Dokuments explizit dazu aufgefordert werden, Makros zu aktivieren.
- Aktivieren Sie das Makro nicht, wenn Sie ein Bewerbungsschreiben, eine Rechnung oder einen Lieferschein bekommen und danach aufgefordert werden, das Makro zu aktivieren.

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

Die Nutzung und Einbindung privater IT Geräte (Notebooks, Tablets, Handys, private Drucker,…)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. Es dürfen keine betrieblichen Daten in welcher Form auch immer auf privaten Gerten gespeichert werden.

Einzig die Nutzung des Nöku Desktops (https:\\noeku.cloud.com) ist mit privaten Geräten möglich und gestattet. Siehe Punkt 2.1 und 2.2

2.16 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. Streaming von Musik und anderen Formaten ist jedoch aus Gründen der Netzwerkbelastung generell untersagt. 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.