Verfahrensregeln „IT des Departments für Nutzpflanzenwissenschaften“

Präambel

Die Verfahrensregeln „IT des Departments für Nutzpflanzenwissenschaften“ sollen allen beteiligten Parteien helfen, zu den meisten **Fragen im Bereich IT / IT-Betreuung** Orientierung zu bieten. Grundlage hierfür bildet die Informationssicherheitsrichtlinie der Universität Göttingen.

Inhalt

IT-Regeln

IT-Regel 1 - Betreuung der IT-Ausstattung

Alle dienstlich genutzten IT-Systeme am DNPW sind Eigentum der Georg-August-Universität Göttingen und fallen in den Zuständigkeitsbereich der IT-Abteilung des DNPW. Die Betreuung der IT-Systeme obliegt den Mitarbeitern der IT- Abteilung des DNPW.

IT-Regel 2 - Beschaffung von IT-Komponenten

Hard- und Software zum Einsatz in den Netzen des DNPW wird durch die IT-Abteilung des DNPW beschafft. Anderweitig beschaffte Komponenten können nicht angeschlossen, installiert, betreut sowie nicht durch das DNPW bezahlt werden. Bestellungen werden nach Genehmigung der zuständigen Abteilungsleitung über das Sekretariat oder das Geschäftszimmer unter Angabe einer Kostenstelle an das Ticketsystem (dnpw-it@uni-goettingen.de) übermittelt. Die weitere

kaufmännische Abwicklung liegt bei der IT-Abteilung des DNPW.

Die Installationen aus bestehenden Repositorien (z. B. Apps aus dem Apple AppStore oder dem Microsoft Store) ist nicht reglementiert. Die Benutzer sind dabei verpflichtet, die Richtlinien der Universität Göttingen (z.B. Richtlinie zum Einsatz von Skype in der Universität Göttingen, IT-Sicherheitsrichtlinie bitte Hyperlinks zu den Richtlinien einfügen) einzuhalten.

IT-Regel 3 - Administratorenrechte

Auf IT-Systemen im DNPW darf nur Software installiert werden, die zur Erfüllung der dienstlichen Aufgaben erforderlich ist.

Die Vergabe von Administratorenrechten erfolgt nach einem 3-stufigen System.

1. Zur Erledigung typischer Aufgaben wie Installation von Software, deren Nutzung auf Dienstrechnern zulässig ist, steht mit der Remotesupport Lösung „AnyDesk“ ein Tool zur zeitnahen und unkomplizierten Ferninstallation durch die IT Abteilung des DNWP bereit.
2. Ist die Aufgabe nicht per Ferninstallation einzurichten, können temporäre Administratorenrechte für die einmalige Erledigung von administrativen Aufgaben angefordert werden. *(Kommentar Herr Wolf: „Muss noch geprüft/eingerichtet werden“)*
3. Kann dem Nutzerbedarf durch 1. und 2. nicht entsprochen werden, können dauerhafte lokale Administratorenrechte gemäß
    a. Richtlinie zur Informationssicherheit der Georg-August-Universität Göttingen / Georg-August-Universität Göttingen Stiftung Öffentlichen Rechts,
    b. fachlicher Einschätzung nur an Personen vergeben, die diese auch als Administratoren im Sinne der Richtlinie zur Informationssicherheit für die Umsetzung spezifischer Administratoren-Aufgaben benötigen.

Zum Erhalt dauerhafter, lokaler Administratorrechte muss ein Antrag mit Begründung der Notwendigkeit gestellt werden. Es können nur Administratorrechte für ein einzelnes IT-System und einen Server beantragt werden.

Für den Erhalt lokaler Administratorrechte bedarf es eines schriftlichen Antrags an die/den IT-Koordinator*in. Inhaltlich erforderlich sind: die Angabe, für welches IT-System (Hostname und MAC-Adresse) die Administratorrechte beantragt werden, in welcher Form der individuelle IT-Bedarf durch Fernwartung und temporäre Administratorrechte nicht abgedeckt ist.

Über den Antrag entscheidet die/der IT-Koordinator*in nach technischer Prüfung. In Zweifelsfällen liegt die Letztentscheidung bei dem/der Direktor*in des DNPW . Die technische Umsetzung der Einrichtung der dauerhaften, lokalen Administratorrechte obliegt der IT-Abteilung des DNPW.

IT-Regel 4 - Eigentum

Dienstrechner sind kein Eigentum der Nutzer und dürfen nach dem Ausscheiden nicht zu privaten Zwecken mitgenommen werden. Sie sind spätestens am letzten Arbeitstag eines Dienstverhältnisses zurückzugeben. Ausnahmen zur Abarbeitung noch weiterlaufender Projekte, für die das jeweilige Gerät zwingend benötigt wird, sind im Ausnahmefall auf begründeten Antrag der jeweiligen Abteilungsleitung hin möglich. Das Gerät muss im Anschluss an die genehmigte Weiternutzung zurückgegeben werden. Mit Zeichnung der sachlichen Richtigkeit wird bestätigt, dass der Kauf (der Ware bzw. der Leistung) wirtschaftlich geboten war, nach den gesetzlichen Vorschriften oder sonstigen Regelungen der Universität, (VOL, Budgetregeln o.ä.) vorgenommen und die Ware respektive Leistung vollständig geliefert wurde und in das Eigentum der Universität übergegangen ist (vgl. Verfahrensregel „Sachlich und rechnerisch richtig“ 1.2 Inhalt der sachlichen Richtigkeit).

IT-Regel 5 - Anwenderqualifizierung

Die Mitarbeiter sind aufgabenspezifisch für die am Arbeitsplatz eingesetzten IT-Verfahren zu schulen. Schulungsziele sind:

a) sicherer Umgang mit der Anwendung,

b) Sensibilisierung für Fragen der IT-Sicherheit,

c) Förderung der Selbsteinschätzung bei auftretenden Problemen (Wann sollten Experten hinzugezogen werden?),

d) Kenntnis über bestehende Bestimmungen,

e) Kenntnis über die Anforderungen des Datenschutzes.

Die Schulungsmaßnahmen werden generell durch das Schulungsangebot der Georg-August-Universität abgedeckt. Der Schulungskatalog ist bei der Abteilung 5 - Personalentwicklung einzusehen:

Abteilung 5 - Personalentwicklung

Herzberger Landstraße 2

37085 Göttingen

personalentwicklung@uni-goettingen.de

Im Bereich der IT-Sicherheit bietet der Informationssicherheitsbeauftragte (https://www.uni-goettingen.de/de/it-sicherheit/52733.html) oder die IT-Abteilung des DNPW Schulungen und Unterweisungen für die Mitarbeiter des DNPW an.

IT-Regel 6 - IT-Koordinator*in

IT-Koordinator*in der Departments ist eine Person mit Leitungsbefugnis im Auftrag des Vorstandes. Die Aufgaben der/des IT-Koordinator*in bestehen in der Koordination und Entscheidung übergreifender Fragen incl. der Entscheidung über die Vergabe sicherheitsrelevanter und Administratorenrechte. Hierzu führt die/ der IT-Koordinator*in regelmäßig einen Jour fixe mit der IT-Abteilung des DNPW durch und ist Ansprechpartner*in für alle Fragen, die über die technische Ebene hinausgehen. Die/der IT- Koordinator*in wird vom Vorstand gewählt und bei Bedarf neu bestimmt.

IT-Regel 7 - Ausmusterung / Weiterverkauf und Entsorgung

Die IT-Abteilung des DNPW wird in der Regel durch Fehlfunktionen von Geräten auf defekte oder veraltete IT-Komponenten (Hard- bzw. Softwareprodukte) aufmerksam. Die Mitarbeiter der IT prüfen die weitere Einsatzfähigkeit oder treffen die Entscheidung zur Ausmusterung (Verschrottung). Diese Geräte werden von der IT-Abteilung des DNWP eingezogen, und es werden von der jeweiligen Abteilung entsprechende Absetzungsanträge erstellt und weitergeleitet.

Die IT-Abteilung des DNPW ist für die Entfernung sämtlicher relevanten und vertraulichen Daten auf entsprechenden Medien (Festplatten etc.) verantwortlich. Entweder werden die Datenträger physisch zerstört oder mit entsprechender Software gelöscht / überschrieben. Damit ist eine Wiederherstellung von relevanten Daten nicht mehr möglich.

Die nicht mehr nutzbaren Geräte werden zur fachgerechten Entsorgung gesammelt und in Abständen an die Stabsstelle Sicherheit übergeben oder nach beidseitiger Absprache direkt durch eine Firma (Schrottverwertung) abgeholt.

Spezifische Kennzeichen (Inventaraufkleber, Namensschilder etc.) werden vorher von der Abteilung IT entfernt. Sollte es zu einem sogenannten Wiederverkauf an einen Angehörigen der Universität Göttingen kommen, sind folgende Dinge zu beachten:

/ Steht der Arbeitsaufwand zur Bereitstellung im angemessenen Verhältnis zum erzielten Verkaufspreis?

  Beispiel: ein ausgemusterter PC wird im Schnitt für 40 € verkauft. Die vorab notwendigen Arbeiten (Löschung der Festplatte, Prüfung der Grundfunktion, evtl. Suche nach Dokumentationen, Verkaufsaktion, Buchung von Belegen etc.) würden diesen Betrag weit übersteigen.

/ Der Käufer muss schriftlich bestätigen, dass er Bastelware ohne Gewährleistungsansprüche ersteht und für eine entsprechende umweltgerechte Entsorgung dieser Geräte verantwortlich ist.

/ Dem Käufer ist das Risiko beim Einsatz von ausgemusterter Elektroware (Stromschlag, Brand durch Kurzschluss) anzuzeigen.

IT-Regel 8 - Datensicherung

Sämtliche relevante Daten / Informationen sind Eigentum der Universität Göttingen und müssen von den Nutzerinnen und Nutzern auf Speicherlösungen der GWGD (ownCloud, P-Laufwerke oder Gruppenlaufwerke) gespeichert werden. Da bei PC-Problemen die IT-Systeme unter Umständen eine neue Basisinstallation erhalten, würden dadurch lokale Daten unwiederbringlich verloren gehen, wenn diese nicht auf Speicherlösungen der GWDG gespeichert werden.

IT-Regel 9 - Das IT-System

(1) Zur Erreichung eines angemessenen Sicherheitsniveaus für IT-Systeme ist eine Standardisierung der technischen Ausstattung und der Konfiguration umzusetzen.

(2) Durch die zentrale Bereitstellung von IT-Diensten durch die IT-Abteilung des DNPW werden die Einrichtungen entlastet, um ihre eigentlichen Aufgaben besser erfüllen zu können. Durch eine Zentralisierung von IT-Diensten wird eine verbesserte IT-Sicherheit erreicht.

(3) Die Einrichtungen müssen auf zentrale IT-Dienste zurückgreifen. (z. B. Domänen-Dienste, Laufwerke, uvm.)

(4) Auf allen Arbeitsplatzrechnern ist grundsätzlich ein Virenscanner einzurichten, der automatisch alle eingehenden Daten und alle Dateien überprüft. Regelmäßig (automatisiert) ist der Virenscanner inkl. der Signaturen zu aktualisieren.

Wird auf einem System schädlicher Programmcode entdeckt, muss dies den IT-Beauftragten des DNPW gemeldet und das Ergebnis der eingeleiteten Maßnahmen dokumentiert werden.

In regelmäßigen Abständen sowie bei konkretem Bedarf oder Verdacht ist eine Suche nach Schadprogrammen auf allen bedrohten IT-Systemen vorzunehmen.

(5) Anwendungen - insbesondere Netzanwendungen wie Mailprogramme und WWW- Browser - sind sicher zu konfigurieren.

(6) Anwendungen sind - soweit technisch möglich - ohne besondere Privilegien im Betriebssystem (Administratorrechte) auszuführen.

(7) Zur Reduzierung des Diebstahlrisikos sind Diebstahl-Sicherungen überall dort einzusetzen, wo nicht unwesentliche Werte zu schützen sind.

(8) Datenträger mit Forschungsdaten und personenbezogenen Daten sind in angemessener Weise zu schützen.

(9) Nutzerinnen und Nutzer dürfen nur mit den Zugriffsrechten ausgestattet werden, die für die Erledigung seiner/ihrer Dienstaufgaben erforderlich sind. Insbesondere sind Arbeiten, für die nicht zwingend erhöhte Privilegien benötigt werden, keinesfalls mit privilegierten Nutzerkonten („Administrator“, „root“ o.a.) vorzunehmen.

(10) Jeder Person sollte nur ein Nutzerkonto zugeordnet sein. Die Zuordnung von mehreren Nutzerkonten zu einer Person innerhalb eines IT-Systems sollte nur in begründeten Ausnahmefällen erlaubt sein, wie beispielsweise für Systemadministratoren.

Die Einrichtung und Freigabe eines Nutzerkontos darf nur in einem geregelten Verfahren erfolgen. Die Einrichtung und Freigabe ist zu dokumentieren

IT-Regel 10 - Konsequenzen und Sanktionen bei Verstößen

Konsequenzen und Sanktionen bei Verstößen werden gemäß den universitären Richtlinien gehandhabt.

IT-Regel 11 - Nutzerkonten

(1) Alle dienstlich genutzten IT-Systeme (einschließlich Smartphones) sind so einzurichten, dass nur berechtigte Personen die Möglichkeit haben, auf diese zuzugreifen. Infolgedessen ist zunächst eine Anmeldung mit einem geeigneten Authentisierungsverfahren (Passwort, biometrische Verfahren o.ä.) erforderlich.

(2) Die Vergabe von Nutzerkonten für die Arbeit an IT-Systemen muss personenbezogen erfolgen. Die Arbeit unter dem Nutzerkonto einer anderen Person ist unzulässig.

(3) Vertretungen sind nicht durch Weitergabe von Zugangsdaten personenbezogener Nutzerkonten, sondern durch geeignete Rechtevergaben zu organisieren.

(4) IT-Anwendern und Anwenderinnen ist untersagt, die für das Authentisierungsverfahren erforderlichen Zugangsdaten weiterzugeben.

(5) Die Verwaltung der Nutzerkonten des DNPW obliegt der IT-Abteilung des DNPW. Als Verwaltung werden die folgenden Aufgaben zusammengefasst.

/ Nutzerkonten ausgeben

/ Kennwörter zurücksetzten

/ Nutzerkonten von ausgeschiedenen Mitarbeiterinnen und Mitarbeitern löschen

(6) Die Laufzeit eines Accounts richtet sich nach der Tätigkeit der Person in der Universität. Folgende Tabelle zeigt die Abhängigkeit zwischen Tätigkeit und Laufzeit des Accounts nach dem Ausscheiden.

Personenkreis	**Laufzeit nach Austritt**	**Sperrung im SAP**
Professor/innen (Pensionierung)	kein Ablaufen	sofort
Professor/innen (Wechsel der Hochschule)	1 Jahr	sofort

Wiss. Mitarbeiter/innen	6 Monate	sofort
Mitarbeiter/innen TV	Deaktivierung zum Austrittsdatum	sofort