

Dienstanweisung

für Benutzer

(Benutzer-Dienstanweisung)

über den Einsatz von Informationstechnik

im

Landesbetrieb Landwirtschaft Hessen (LLH)

GLIEDERUNG

Inhalt

Präambel

1. Allgemeines	3
1.1 Anwendungsbereich	3
1.2 Begriffsbestimmungen	3
2. Zuständigkeiten und Verantwortung.....	4
3. Berechtigungen	5
3.1 Benutzerkennungen, Zugriffsberechtigungen	5
3.2 Administration.....	5
4. Systeme	6
4.1 Zentrale IT-Systeme	6
4.2 Dezentrale IT-Systeme	6
4.3 Mobile Geräte (Notebooks, Handhelds, etc.).....	6
4.4 Datensicherung durch den Benutzer	6
5. Nutzungsregelungen für IT-Anwender	7
5.1 Zweckbindung	7
5.2 Grundsätze	7
5.3 Nutzung Internet und E-Mail.....	7
5.4 Umgang mit Passwörtern	8
5.5 Informationspflichten	9
5.6 Fernwartung/Remote-Zugriff	9
5.7 Umgang mit speziellen Medien (z.B. Präsentationsmedien)	9
6. Kenntnisnahme	9
7. Salvatorische Klausel.....	10
8. Schlussbestimmungen.....	10

Anlagen

Präambel

Der LLH stellt allen Mitarbeiterinnen und Mitarbeitern eine leistungsfähige IT-Infrastruktur (Hard- und Software) zur Verfügung - soweit diese für die wahrgenommene Funktion /Aufgabe benötigt wird.

Für den Umgang mit diesen dienstlichen "Arbeitsmitteln" bzw. deren Einsatz im LLH bedarf es einiger Regeln. Die Einhaltung dieser Regeln dient zum Einen der Datensicherheit bei den Anwenderinnen und Anwendern. Gleichzeitig wird der LLH in die Lage versetzt, alle im Land Hessen vorgesehenen Standards der IT-Sicherheit einzuhalten.

Die nachstehenden Regelungen dienen der Information und Orientierung aller Kolleginnen und Kollegen des LLH.

1. Allgemeines

1.1 Anwendungsbereich

Mit dieser Dienstanweisung wird der Einsatz der Informationstechnik (IT) im Landesbetrieb Landwirtschaft Hessen geregelt.

Die Dienstanweisung dient der Sicherheit der IT-Anwendungen unter Beachtung der Grundsätze ordnungsgemäßer Datenverarbeitung. Dabei sind die für die IT geltenden Rechtsvorschriften und Richtlinien der EU, des Bundes und des Landes Hessen in der jeweils aktuellen Fassung zu berücksichtigen. Insbesondere gilt dies für die Datenschutzgesetze sowie die Erlasse zum IT- Grundschutz und der IT-Sicherheit.

1.2 Begriffsbestimmungen

Unter „Einsatz der IT“ sind alle Aufgaben zu verstehen, die im Zusammenhang stehen mit

- der Entwicklung oder Erweiterung von IT-Anwendungen,
- der Erfassung / Eingabe von Daten¹,
- der Datenannahme¹,
- der maschinellen Verarbeitung (Speicherung, Übermittlung, Löschung und Veränderung) von Daten²,
- der Datenausgabe / -anzeige,
- der Datenübermittlung / -fernübertragung und
- der Nutzung des E-Mail-Dienstes und des Internet.

Weitere Begriffsdefinitionen/Abkürzungen:

- | | |
|---------------------|---|
| ■ IT | Informationstechnik |
| ■ DV | Datenverarbeitung |
| ■ APC | Unter APC (Arbeitsplatzcomputer) werden Einplatzsysteme verstanden, die auch in Netzen betrieben werden können (PC, Notebook, Thin-Client, etc.). |
| ■ PC | Personal Computer (dt. <i>persönlicher Computer</i>) ist ein Einzelplatzrechner, der im Gegensatz zu einem Großrechner von einer einzelnen Person (daher <i>persönlich</i>) bedient, genutzt und gesteuert werden kann. |
| ■ Notebook / Laptop | Ein Notebook (engl. <i>notebook</i> – Notizbuch) – auch Laptop (engl. <i>laptop</i> – „auf dem Schoß“) ist ein kleiner, tragbarer Computer. |
| ■ Thin-Client | Thin Client (engl. wörtlich "dünner Dienstanwender") bezeichnet innerhalb der elektronischen Datenverarbeitung eine Anwendung oder einen Computer als Endgerät eines Netzwerkes, dessen funktionale Ausstattung auf die Ein- und Ausgabe beschränkt ist. |
| ■ USB-Stick | Universal Serial Bus (universelle serielle Schnittstelle, kurz USB), USB-Stick (USB-Stift oder USB-Speicherstab) ist ein deutscher Scheinanglizismus, der in englischen Sprachgebieten nicht verwendet wird. Es handelt sich um ein Speichermedium in einem kompakten Gehäuse. |
| ■ Handhelds | Ein Handheld bzw. Handgerät ist ein tragbares, elektron. Gerät mit eigener Stromversorgung für untersch. Anwendungen. Es ist so klein und leicht, dass es bei der Benutzung in nur einer Hand gehalten werden kann, daher die Bez. <i>Handheld</i> (von engl. <i>in der Hand gehalten</i>). Handhelds sind eine Untergruppe der Mobilgeräte. |

¹ Es ist die technische Erfassung/ Eingabe und Datenannahme gemeint, nicht die fachliche.

² Maschinelle Verarbeitung von Daten ist die Verarbeitung durch und mit einem Rechnersystem

- **Server** Der Begriff **Server** (engl. für *Diener*) bezeichnet entw. eine Software (Programm) im Rahmen des Client-Server-Modells oder eine Hardware (Computer), auf der diese Software im Rahmen des Konzepts abläuft.
Ein **Server (Software)** ist ein Programm, das mit einem anderen Programm, kommuniziert, um ihm Zugang zu speziellen Dienstleistungen zu verschaffen. Ein **Server (Hardware)** ist ein Computer, auf dem ein oder mehrere Server (Software) laufen.
- **Makro** Ein **Makro** ist ein Programm, das eine fest vorgegebene Folge von Befehlen, Aktionen oder Tastaturcodes enthält. Alle Anweisungen des Makros werden automatisch ausgeführt, wenn das Makro aufgerufen wird.
- **Remote Zugriff** (von engl. *remote*, „entfernt, fern“) ist ein Fernzugriff auf einen Rechner innerhalb eines Netzwerkes. Der Remote-Zugriff wird zur Darstellung und Steuerung eines entfernten Rechners genutzt.
- **Benutzerprofil** Ein **Benutzerprofil** oder Userprofil ist in der Systemadministration eine Konfiguration in einem Betriebssystem oder Rechnernetz. Diese Konfigurations-Daten werden zentral in einem speziellen Ordner verwaltet. Das Benutzerprofil enthält die Benutzerrechte eines Benutzers.
- **ZDA** Zentrale Datenablage (kurz ZDA) des LLH
- **ZEM** Zentrale E-Mail-Plattform
- **E-Mail** **E-Mail** (kurz Mail, von: „electronic mail“; dt. „elektronische Post“ oder „elektronischer Brief“) bezeichnet eine auf elektronischem Weg in Computernetzwerken übertragene, briefartige Nachricht.
- **SAP** Die **SAP AG** ist ein großer globaler Softwarehersteller. Die Abkürzung kommt von Systeme, Anwendungen und Produkte (kurz SAP) und wird im Sprachgebrauch für die von SAP entwickelte Standard-Software für die wesentlichen Bereiche FI (Finance - Finanzen), Co (Controlling), MM (Materials Management - Materialverwaltung), HR (Human Resources - Personalverwaltung), SD (Sales and Distribution – Vertrieb und Auftragsverwaltung) und PP (Produktion Planning - Produktionsplanung) benutzt.
- **HZD** Die **Hessische Zentrale für Datenverarbeitung** (HZD) ist der IT-Dienstleister für die hessische Landesverwaltung.
- **HMdluS** Hessisches Ministerium des Innern und für Sport
- **AL** Abteilungsleiter
- **FG** Fachgebiet
- **FGL** Fachgebietsleiter

2. Zuständigkeiten und Verantwortung

Die fachliche Zuständigkeit ist wie folgt definiert:

- **Fachgebiet „Informationstechnik“:**
 - die Beschaffung IT-Hardware und Software, IT-Dienstleistungen (→ Planung und Spezifikation des Bedarfs)
 - die Gewährleistung der Funktionsfähigkeit
- **HZD:**
 - die Speicherung und maschinelle Verarbeitung sowie die Verfügbarkeit der Daten bei zentraler Datenhaltung entsprechend den getroffenen Vereinbarungen (z.B. ZDA, ZEM, SAP)
- **Fachgebiete:**
 - fachliche Definitionen für die Erstellung oder Veränderung von IT-Anwendungen und Meldung des Bedarfs von IT-Technik in Zusammenarbeit mit dem FG „Informationstechnik“
- **Benutzer:**
 - Speicherung und maschinelle Verarbeitung² sowie die Verfügbarkeit der Daten bei dezentraler Datenhaltung (z.B. auf PC-Festplatten)

3. Berechtigungen

3.1 Benutzerkennungen, Zugriffsberechtigungen

Für die Vergabe der Zugriffsrechte auf die Netzwerkinfrastruktur³ ist das FG „Informationstechnik“ zuständig.

Die Leitungen der Fachgebiete legen entsprechend der Aufgaben die Erteilung und Entziehung der Zugriffsrechte der IT-Benutzer für die Ordnerstruktur/zentrale Datenablage⁴ fest. Auf eine zeitnahe Löschung von nicht mehr benötigten Zugriffsrechten⁵ ist zu achten.

Die sachgerechte Vergabe der Zugriffsberechtigungen muss nachvollziehbar und zwischen den Organisationseinheiten abgestimmt sein. Die Einrichtung der Zugriffsberechtigungen wird von den hierfür zuständigen Mitarbeiterinnen und Mitarbeitern des Fachgebietes „Informationstechnik“ vorgenommen.

Das vorsätzliche Ausprobieren, Ausforschen oder die Benutzung fremder Zugriffsberechtigungen ist unzulässig.

Das vorsätzliche Ausprobieren, ob weitere Dienste oder Zugriffsrechte als die Erlaubten genutzt werden können, ist ebenfalls verboten.

3.2 Administration

Für die Administration wird eine gesonderte Dienstanweisung (Administratoren-Dienstanweisung) abgeschlossen, in der die Verantwortlichkeiten definiert sind.

3.3 Zugriff auf Benutzerkonten und Postfächer bei ungeplanter Abwesenheit

Bei geplanter Abwesenheit (z.B. Urlaub, Gleittag, Dienstreise usw.) ist eine Vertretung des Nutzers vorzusehen. Die Vorgesetzte bzw. der Vorgesetzte organisiert insbesondere für den Fall der ungeplanten Abwesenheit eines Beschäftigten einen Zugriff auf dessen Benutzerkonto, um die Aufrechterhaltung eines ordnungsgemäßen dienstlichen Ablaufs zu gewährleisten. Die verbindliche Vorgabe ist der Anlage „Verfahrensbeschreibung zur Öffnung von E-Mail-Postfächern und Benutzerkonten“ zu entnehmen.

Diese Möglichkeit besteht nicht für die Benutzerkonten folgender Gremien:

- Personalrat (inkl. Nachrücker)
- Jugend- und Auszubildendenvertretung
- Schwerbehindertenvertretung
- Frauenbeauftragten
- Datenschutzbeauftragten

Benutzerkonten und Postfächer für die benannten Gremien sind in jedem Fall so einzurichten, dass keine anderen Personen Zugang zu den Daten haben.

³ Mit Netzwerkinfrastruktur ist das gesamte Netzwerk mit allen Komponenten gemeint.

⁴ Mit der Ordnerstruktur ist die zentrale Datenablage (ZDA -> Laufwerk P) gemeint.

⁵ z.B. bei Praktikantenverträgen, Werkverträgen, ausscheidenden Mitarbeiter o.ä.

4. Systeme

4.1 Zentrale IT-Systeme

Zu den zentralen IT-Systemen gehört das gesamte, im Rahmen des Client-Server-Betriebs für die zentrale Datenhaltung und –verarbeitung, eingesetzte Rechnerumfeld sowie das Netzwerk-Umfeld. Zentrale IT-Systeme werden von der HZD oder vom Fachgebiet „Informationstechnik“ betreut und verwaltet.

Alle auf den zentralen IT-Systemen durchgeführten Arbeiten werden – soweit technisch möglich – auf Maschinenprotokollen festgehalten. Die Unterlagen bzw. Maschinenprotokolle können auf Antrag des Fachgebietes „Informationstechnik“ bei der HZD eingesehen werden. Der Personalrat des LLH wird auf Wunsch über Ziele, Art und Anzahl der Anfragen informiert. Die Protokolle können auch durch den Personalrat eingesehen werden.

4.2 Dezentrale IT-Systeme

Dezentrale IT-Systeme sind lokal oder am Netz betriebene Arbeitsstationen (z.B. stationäre und mobile PCs, Drucker, Handhelds, auch Netzwerkplatten, etc.).

4.3 Mobile Geräte (Notebooks, Handhelds, etc.)

Bei mobilen Geräten ist/sind vom Benutzer:

- in regelmäßigen Abständen eine Datensicherung auf die zentrale Datenablage (ZDA) durchzuführen.

Bei mobilen Geräten ist/sind vom FG „Informationstechnik“:

- die Einstellungen zum Netzwerk aus Sicherheitsgründen so konfiguriert, dass diese nicht an anderen Standorten oder in Netzen anderer Institutionen funktionieren. Ausnahmen von dieser Regel dürfen nur vom FG „Informationstechnik“ eingerichtet werden.
- verändernde Zugriffe auf die Betriebssystemebene und auf die Konfigurationen sonstiger IT-Komponenten sowie der Einsatz nicht freigegebener Software technisch zu verhindern.
- eine wirksame Zugriffsschutzmaßnahme (Einsatz von Passwörtern oder Schutzsoftware wie z.B: Safeguard) eingerichtet.
- der Einsatz eines geeigneten Virenschutzes vorzusehen.

4.4 Datensicherung durch den Benutzer

Werden Daten auf lokalen Speichern ⁶ (Festplatten, USB-Sticks usw.) abgelegt, liegt die Verantwortung für die Datensicherung beim Benutzer/in. Die Daten müssen regelmäßig gesichert werden. Das FG „Informationstechnik“ unterstützt bei der Umsetzung und steht beratend für individuelle Lösungen zur Verfügung. Die Sicherungsbestände sind vor unbefugter Einsichtnahme bzw. gegen Verlust geschützt zu verwahren.

⁶ Lokale Speicher sind alle Speicher, die nicht über das Netz verwaltet werden. Also alle Speicher, die in der Verantwortung des Benutzers liegen

5. Nutzungsregelungen für IT-Anwender

5.1 Zweckbindung

Der/m Benutzer/in ist es grundsätzlich untersagt,

- dienstliche Hard- und Softwareprodukte oder dienstliches DV-Zubehör privat zu nutzen,
- privat genutzte Hardware, Software oder privat genutztes DV-Zubehör im Dienstbetrieb einzusetzen bzw. mit dienstlicher Hardware zu verbinden,
- Systemveränderungen an Hard- und Software ohne Einbeziehung des FG „Informationstechnik“ vorzunehmen.⁷

5.2 Grundsätze

- Es dürfen nur dokumentierte, durch das FG „Informationstechnik“ freigegebene und aktuell gültige Programme (dazu gehören z.B. auch Makros, s.⁸), eingesetzt werden.
- Es dürfen nur vom Fachgebiet „Informationstechnik“ installierte Hard- und Softwarekomponenten verwendet werden.
- Für die Installation⁸ und Anpassung der Hardware sowie System- und Anwendungssoftware ist ausschließlich das Fachgebiet „Informationstechnik“ zuständig. Änderungen an den Systemeinstellungen (Installation, Deinstallation, Änderungen an der Konfiguration etc.) sind nur durch die zuständigen Administratoren zulässig.

Abweichungen von den Grundsätzen bedürfen in jedem Fall der Zustimmung des FG „Informationstechnik“ und sind mit den zuständigen FGL abzustimmen.

5.3 Nutzung Internet und E-Mail

- Internet und E-Mail sind unverzichtbare Informations- und Kommunikationssysteme, die allen Mitarbeiterinnen und Mitarbeitern (mit APC) für dienstliche Zwecke uneingeschränkt zur Verfügung stehen⁹.
- E-Mail- und Internetnutzung sollen grundsätzlich nur zu dienstlichen Zwecken erfolgen.

⁷ Daraus folgt, dass es zur Sicherung der Landesnetze unerlässlich ist, alle unmittelbaren "Verbindungen" zwischen privaten und dienstlichen IT-Systemen zu unterlassen. Die Problematik des Schutzes des HCN-Netzes des Landes vor "Angriffen" von Außen (Viren, Trojaner, Hacker) setzt hier hohe Anforderungen.

Bitte beachten Sie diese Regeln - auch zu Ihrer eigenen Sicherheit - sehr genau und setzen Sie im Dienst ausschließlich dienstliche Komponenten (USB-Sticks, externe Festplatten, Drucker etc.) ein.

⁸ Die Installation von Programmen ist nur (ausschließlich) durch das FG „Informationstechnik“ erlaubt. Dies gilt auch für (selbst erstellte) Excel-Macros. Bereits diese können dazu führen, dass andere installierte Programme nicht mehr ordnungsgemäß laufen. Die Testung eines Excel-Macros durch das FG „Informationstechnik“ dauert nur kurze Zeit und schafft die für den Einsatz erforderliche Sicherheit.

⁹ Das Internet ist nicht nur eine Informationsquelle, die in der Arbeitswelt nicht mehr entbehrt werden kann. Es bietet auch immer wieder Anlass für kontroverse Diskussionen. Allen Kolleginnen und Kollegen ist dies auch bekannt und bewusst. Daher dieser Appell: bitte vermeiden Sie alle Zugriffe, die gegen das Strafrecht, Persönlichkeitsrechte, Urheberrechte oder gegen den Datenschutz verstoßen. Ebenso sind Zugriffe verboten, wenn diese diskriminierende, beleidigende, verleumderische, menschenverachtende, verfassungsfeindliche, gewaltverherrlichende, rassistische, sexistische oder pornographische Inhalte darstellen. Der LLH wird gegen Mitarbeiterinnen und Mitarbeiter, die diese Grundsätze verletzen, mit allen dienst- und arbeitsrechtlichen Konsequenzen vorgehen (müssen).

- Die private Nutzung¹⁰ ist nur in geringfügigem Umfang gestattet, wenn dienstliche Belange nicht entgegenstehen und die Nutzerin bzw. der Nutzer die in der Anlage befindliche Einwilligungserklärung zuvor schriftlich abgegeben hat. Dienstliche Belange stehen insbesondere entgegen, wenn die Nutzung geeignet ist, den Dienstbetrieb zu beeinträchtigen, den Interessen und dem Ansehen des Landes zu schaden, die Verfügbarkeit der IT-Systeme für dienstliche Zwecke beeinträchtigt sein kann oder die Nutzung gegen geltendes Recht, insbesondere gegen persönlichkeitsrechtliche, datenschutzrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstößt.
- Wird die Einwilligung zur privaten Nutzung von Internet und E-Mail (Anlage) nicht abgegeben, ist ein privater Gebrauch von Internet und E-Mail ausdrücklich untersagt. Die Einhaltung des Verbots wird überwacht. Die Gestattung der Nutzung zu privaten Zwecken kann jederzeit eingeschränkt oder widerrufen werden.
- In keinem Fall darf die Nutzung der dienstlichen E-Mail-Adresse zu nennenswerten Betriebsablaufstörungen führen.
- Zu privaten Zwecken ist die Nutzung von Internet-Diensten in geringfügigem Umfang, sofern dienstliche Belange nicht entgegen stehen, zulässig. Unzulässig sind jedoch insbesondere das Herunterladen von Programmen und anderen ausführbaren Dateien, die Teilnahme an Foren, Netz-, Onlinespielen und Auktionen, sowie die Verfolgung gewerblicher Zwecke. In jedem Fall unzulässig ist das Aufrufen oder Herunterladen diskriminierender, beleidigender, verleumderischer, menschenverachtender, verfassungsfeindlicher, gewaltverherrlichender, rassistischer, sexistischer, pornographischer oder anderer, außerhalb des gesetzlichen Rahmens befindlicher Inhalte.
- Die HZD als Internetbetreiber führt ein Zugriffsprotokoll. Diese Auswertungen können in begründeten Fällen von der HZD eingefordert werden.
- Websites, die einen Datenstream (z.B: Webradio usw.) erzeugen, sind zu vermeiden (hohe Netzbelastung).

5.4 Umgang mit Passwörtern

- Das persönliche Passwort bestimmt der Benutzer selbst. Es darf keine Rückschlüsse auf seinen Besitzer zulassen und ist vertraulich zu behandeln.
- Kann nicht ausgeschlossen werden, dass ein Unbefugter Einblick in das Passwort erhalten hat, ist dieses sofort zu ändern. Darüber hinaus sind persönliche Passwörter nach technischer Vorgabe zu ändern.
- Die PC-Benutzer müssen durch den gewissenhaften Umgang mit ihrem Passwort sicherstellen, dass ihre Zugriffsberechtigung nicht von Unberechtigten benutzt werden kann. Eine Weitergabe der Benutzerkennung und des Passwortes an Dritte ist unzulässig.
- Soweit technisch möglich, sind die Anforderungen an den Umgang mit Passwörtern systemseitig einzurichten (z.B. Passwortlänge, Historie, Änderungsintervall usw.). Vorgaben des Landes Hessen (HZD) sind einzuhalten.

¹⁰ Die allgemeinen Regeln zur privaten Nutzung des Internets und die private E-Mail-Nutzung in der Dienststelle werden vom HMdIuS definiert.

5.5 Informationspflichten

Alle sicherheitsrelevanten Ereignisse (z.B. unerklärliches Systemverhalten, Verlust oder Veränderung von Daten und Programmen, Verfügbarkeit nicht ausdrücklich freigegebener Dienste, Verdacht auf Missbrauch der eigenen Benutzerkennung, Alarmmeldungen der Virensoftware usw.) sind sofort dem Fachgebiet „Informationstechnik“ zu melden. Eigene Aufklärungsversuche sind zu unterlassen¹¹.

5.6 Fernwartung/Remote-Zugriff

Bei allen Anwenderinnen und Anwendern, die im Netz arbeiten, besteht die Möglichkeit einer Fernwartung (Remote-Zugriff) mit Zustimmung des/r Nutzers/in. Im Hinblick auf eine schnelle und effiziente "Vor-Ort-Betreuung" soll diese Möglichkeit zukünftig verstärkt genutzt werden. Weitere Einzelheiten werden in der "Administratoren-Dienstanweisung" beschrieben.

5.7 Umgang mit speziellen Medien (z.B. Präsentationsmedien)

Für den Umgang mit speziellen Medien (wie z.B. USB-Sticks, Präsentationsnotebooks usw.) werden gesonderte Merkblätter zur Verfügung gestellt, die den Umgang mit diesen Medien regeln.

6. Kenntnisnahme

Alle Kolleginnen und Kollegen erhalten einen Ausdruck dieser Dienstanweisung und bestätigen den Erhalt sowie die Einhaltung durch ihre Unterschrift.

Bei schuldhafter Zuwiderhandlung entscheidet die Dienststellenleitung unter Beteiligung der Gremien des LLH über arbeitsrechtliche oder disziplinarische Maßnahmen.

¹¹ Der LLH ist mit "seiner" IT ein Teil des IT-Systems des Landes Hessen. Die dafür eingesetzten Server stehen in der HZD. Bitte nehmen Sie die Informationspflichten gegenüber dem FG „Informationstechnik“ sehr ernst. Nur Ihre Rückmeldungen versetzen die "IT" in die Lage, Fehler rechtzeitig zu erkennen und ggf. gemeinsam mit der HZD zu beseitigen.

7. Salvatorische Klausel

Sollten eine oder mehrere Bestimmungen dieser Dienstanweisung ganz oder teilweise rechtsunwirksam sein, so wird dadurch die Gültigkeit der übrigen Bestimmungen nicht berührt. An die Stelle der rechtsunwirksamen Bestimmungen tritt rückwirkend eine inhaltlich möglichst gleiche Regelung, die dem Zweck der gewollten Regelung am nächsten kommt.

8. Schlussbestimmungen

Diese Dienstanweisung tritt am in Kraft.

Änderungen und Ergänzungen sind jederzeit möglich und werden schriftlich bekannt gegeben.

Kassel, den

(Direktor)

ANLAGE: „Kenntnisnahme und Einwilligungserklärung“

Nachname:	Vorname:
Fachgebiet:	

Kenntnisnahme der Benutzer-Dienstanweisung

Die Dienstanweisung für Benutzer (Benutzer-Dienstanweisung) über den Einsatz von Informationstechnik im Landesbetrieb Landwirtschaft Hessen (LLH) habe ich zur Kenntnis genommen und werde die dort gemachten Vorgaben beachten.

Ort, Datum

Unterschrift

Einwilligungserklärung zur privaten Nutzung von Internet- u. E-Mail

Ich möchte die von meiner Dienststelle zur Verfügung gestellten Internet- und E-Mail-Dienste in geringfügigem Umfang auch für private Zwecke nutzen.

Ich willige ein, dass mein privater E-Mail- und Internetverkehr in demselben Maße wie mein dienstlicher E-Mail- und Internetverkehr automatisch protokolliert wird. Ich bin damit einverstanden, dass die Protokolldaten temporär gespeichert werden und stichprobenartig überprüft werden können. Bei einem konkreten Verdacht einer missbräuchlichen Nutzung können alle vorhandenen Protokolle zur personenbezogenen Auswertung verwendet werden und die Anonymität kann auch im Falle der Internetnutzung aufgehoben werden.

Ich gestatte ferner, dass meine privaten E-Mails bei möglicher Verseuchung mit Viren oder anderen Schadprogrammen sowie an mich adressierte unerwünschte oder unverlangt zugehende E-Mails – sog. Spam-Mails – automatisiert herausgefiltert und ggf. nicht zugestellt werden. Mir ist bekannt, dass dabei auch privat erwünschte E-Mails irrtümlich durch den Spamfilter ausgesondert werden können.

Sollten im Fall meiner Abwesenheit vom Arbeitsplatz an mich adressierte E-Mails an meine Vertretung weitergeleitet werden oder sie Zugriff auf mein Postfach nehmen, so billige ich das. Meine Vorgesetzte/ mein Vorgesetzter organisiert insbesondere für den Fall der ungeplanten Abwesenheit einen Zugriff auf mein E-Mail-Konto, wenn dies für einen ordnungsgemäßen betrieblichen Ablauf nötig sein sollte. Mir ist bewusst, dass dabei auch private E-Mails anderen Personen zur Kenntnis gelangen können.

Mir ist bekannt, dass die Gestattung der Privatnutzung von E-Mail und Internet jederzeit eingeschränkt oder widerrufen werden kann. Auch ich kann diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Ab dem Zeitpunkt des Widerrufs darf ich den Internetzugang und den E-Mail-Dienst dann nicht mehr für private Zwecke nutzen.

Diese Erklärung ersetzt alle bisherigen Einwilligungserklärungen, die zur Nutzung von E-Mail und/oder Internetdiensten abgegeben worden sind.

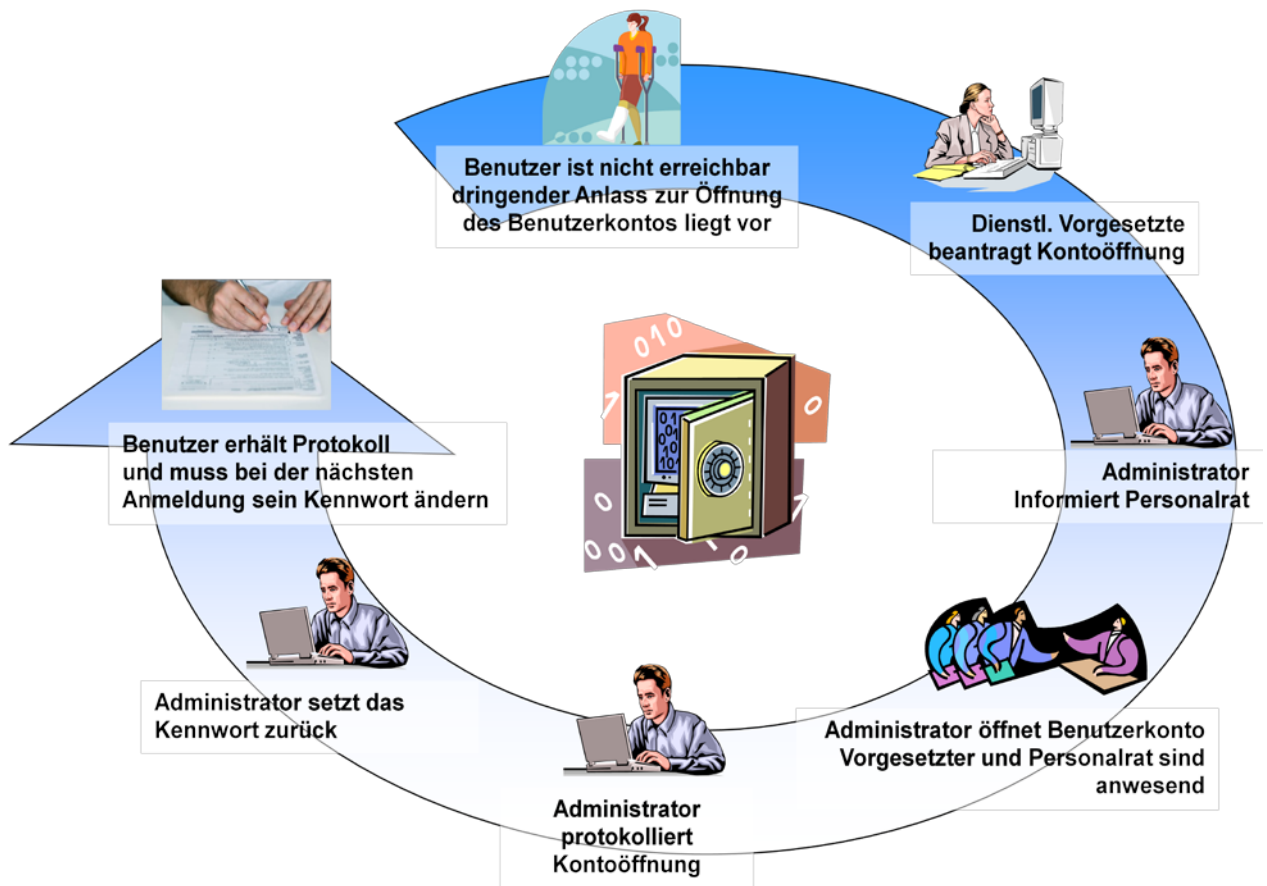
Die Einwilligungserklärung wird in meine Personalakte aufgenommen.

Ort, Datum



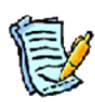
Unterschrift

ANLAGE: „Verfahrensbeschreibung zur Öffnung von E-Mail-Postfächern und Benutzerkonten“

Beschreibung der verbindlichen Vorgabe zur Öffnung von Benutzerkonten und Postfächern:



Erläuterung Benutzerkonto öffnen

Benutzer 	Nicht verfügbar: Auf das Konto eines Benutzers muss zugegriffen werden. Der Benutzer ist für längere Zeit nicht verfügbar. Ein dringender Anlass zur Öffnung des Benutzerkontos muss vorliegen. Nächste Anmeldung: Bei der nächsten Anmeldung muss der Benutzer das Kennwort ändern (zwingend)
Dienstl. Vorgesetzte 	Beauftragung: Der direkte dienstliche Vorgesetzte beauftragt die Administration mit der Öffnung des Benutzerkontos.
Administration 	Information: Der Administrator informiert zuerst den Personalrat über die geplante Öffnung des Benutzerkontos. In Anwesenheit des dienst. Vorgesetzten und des Personalrates wird das Benutzerkonto geöffnet. Protokollierung: Die Öffnung des Benutzerkontos wird über ein definiertes Formular protokolliert (s. Anlage „Zugriff auf Benutzerprofil“) das dem Benutzer ausgehändigt werden muss.

