Dienstanweisung

für Administratoren

(Administratoren-Dienstanweisung)

im

Landesbetrieb Landwirtschaft Hessen (LLH)

G L I E D E R U N G

Inhalt

Präambel

Die Einhaltung aller Vorschriften zur IT-Sicherheit ist von der Dienststelle und allen Beschäftigten zu gewährleisten. Alle Beschäftigten tragen die Verantwortung für die ihnen für dienstliche Zwecke überlassenen IT-Geräte.

Darüber hinaus gibt es eine kleine Gruppe von Mitarbeiterinnen/-Mitarbeitern des Fachgebietes „Informationstechnik“, die über weitergehende Berechtigungen und Zugriffsmöglichkeiten verfügen. Diese Gruppe soll hier nicht nur namentlich benannt werden. Die Administratoren-Dienstanweisung beschreibt die Aufgaben und Eingriffsmöglichkeiten der Administratoren und dient damit der Information und Orientierung aller Beschäftigten.

1. Allgemeines

Für die Nutzung der IT-Systeme werden jedem/jeder Nutzer/in die zur Erfüllung seiner/ihrer Aufgaben notwendigen Rechte eingeräumt. Um das Gesamtsystem inkl. Benutzer, Zugriffsrechte usw. zu verwalten, sind besondere Rechte für Administratoren notwendig. Die nachfolgenden Regelungen und Hinweise zeigen die Möglichkeiten und Aufgaben der Administratoren auf und dienen zur Übersicht auch für die Benutzer.

Die Mitarbeiter des Fachgebietes „Informationstechnik“ verfügen zur Verwaltung der Benutzer und der Zugriffsrechte sowie der Soft- und Hardware über entsprechende Kennungen, die mit den benötigten Administratorenrechten ausgestattet sind. Für die Verwaltung von Soft- und Hardware sind Administratoren-Kennungen ("Vor-Ort-Betreuer" mit örtlichen/lokalen Berechtigungen) eingerichtet, diese Kennungen verfügen nicht über Berechtigungen zur Benutzer- und Zugriffsrechteverwaltung. Hierfür existiert eine Administratorengruppe mit umfassenden Berechtigungen, die die Berechtigungen für die Verwaltung der Benutzer-Systeme beinhalten (s. ANLAGE: „Übersichtsliste Administratoren“). Die nachstehenden Aufgaben und Regelungen gelten somit jeweils im Umfang der zugewiesen Berechtigungen.

Die Administratoren unterliegen der Schweigepflicht über die während ihrer Arbeit erhaltenen Informationen über Benutzer und deren Daten. Die Weitergabe dieser Informationen ist nur bei einem nachhaltig begründeten Verdacht eines Gesetzesverstoßes (z.B. bei Missbrauch von IT-Systemen für rechtsradikale oder pornografische Zwecke) unter Einbeziehung des Personalrates und des Datenschutzbeauftragten erlaubt.

Die Benutzer der Administratorenkennungen sind auf ihre Sorgfaltspflicht in Bezug auf die hier benannten Themen hingewiesen und haben eine entsprechende Erklärung dazu unterschrieben (s. ANLAGE: „Verpflichtungserklärung Administrator“).

Die Vorschriften des Hessischen Datenschutzgesetzes (HDSG) (http://www.hessenrecht.hessen.de) sind zu beachten.

1.1 Persönlichkeitsrechte

Bei der Einführung und Nutzung von IT-Diensten ist stets das grundrechtlich geschützte allgemeine Persönlichkeitsrecht der Nutzer/in zu beachten. Es werden geeignete Maßnahmen getroffen, um die Vertraulichkeit und Integrität der Kommunikation zu gewährleisten. Dieses beinhaltet insbesondere das Recht auf informationelle Selbstbestimmung, den Schutz des eigenen Bildnisses, Schutz der Privatsphäre usw.

1.2 Zweckbindung

Personenbezogene Daten, die zum Zwecke der Sicherstellung eines ordnungsgemäßen Betriebs der elektronischen Kommunikationsmittel (z.B. Fehleranalyse und –korrektur, Systemoptimierung einschließlich Kapazitäts-planung) gespeichert werden, werden nur für diese Zwecke verwendet.

Der Zugriff auf elektronisch gespeicherte Daten und deren Weitergabe innerhalb der Administoren ist ausschliesslich im Rahmen der Erledigung von notwendigen IT-fachlichen Aufgaben zulässig.

Die Administrationskennungen dürfen nur zum Zweck der Aufgaben des Fachgebietes „Informationstechnik“ genutzt werden. Jegliche Nutzung der Administrationsrechte zur Verhaltens- und Leistungskontrolle oder zur Beschaffung von Informationen über Benutzerverhalten und deren Daten ist unzulässig. Die Kennungen sind an Personen gebunden und dürfen nicht weitergegeben werden. Somit ist der Einsatz der Administrationskennungen nachvollziehbar.

Sofern zu Zwecken der Fehleranalyse und der Analyse der Systemsicherheit Proto-kolldaten ausgewertet werden, ist die weitere Verwendung der hierbei gewonnenen Informationen ausgeschlossen. Unberührt bleibt die Pflicht zur Meldung und Ahndung strafrechtlich relevanter Tatbestände.

Personenbezogene Daten, die unter Verletzung der Regelungen dieser Dienstanweisung gewonnen oder verarbeitet wurden, sind als Beweismittel ausgeschlossen.

1.3 Der Administrator:

Er ist für die Bereitstellung und Aufrechterhaltung des IT-Betriebes und der Sicherheitsanforderungen verantwortlich und erhält dafür - unter Berücksichtigung seiner Aufgabe - alle notwendigen Werkzeuge und Berechtigungen.

Der Administrator ist innerhalb seines zugewiesenen Bereichs dafür verantwortlich, dass durch wirksame Maßnahmen die Sicherungsziele realisiert werden und ihre Einhaltung kontrolliert werden kann. Die Administratoren werden darauf verpflichtet, die bei der Nutzung der IT-Dienste anfallenden Benutzerdaten nicht zum Zweck der Leistungs- und Verhaltenskontrolle der Beschäftigten zu nutzen. Die Weitergabe von Informationen und jede Form personenbezogener Auswertungen der Verbindungs- und Benutzerdaten über den festgelegten Umfang hinaus sind unzulässig.

Daneben sind sie Ansprechpartner für Systemfragen sowie für Anwenderfragen.

1.4 Geltungsbereich

Diese Dienstanweisung gilt für die beim LLH eingesetzten Administratoren im Bereich des Fachgebietes „Informationstechnik“. Nur die in der Anlage benannten Administratoren dürfen mit den entsprechenden Rechten ausgestattet werden.

Für die Administratoren der HZD gelten eigene Richtlinien. Sie bleiben von den hier getroffenen Regelungen unberührt.

2. Berechtigungskonzept/Datenablage

Als zentrales Verwaltungsmedium der Benutzer- und Zugriffsberechtigung und ihrer Anwendungen kommt der Verzeichnisdienst Active Directory (AD) von Microsoft für Windows 2000/Windows Server 2003 zum Einsatz. Weiterhin ist für die Datenspeicherung eine Ablagestruktur (Ordnerstruktur / zentrale Datenablage) eingerichtet.

2.1 Active Directory

Active Directory ermöglicht es, ein Netzwerk entsprechend der realen Struktur der Dienststelle oder seiner räumlichen Verteilung zu gliedern. Dazu verwaltet es verschiedene Objekte in einem Netzwerk wie beispielsweise Benutzer, Gruppen, Computer, Server, Dateifreigaben und andere Geräte wie Drucker und Scanner und deren Eigenschaften. Mit Hilfe von Active Directory kann ein Administrator die Informationen der Objekte organisieren, bereitstellen und überwachen.

Das Active Directory verwendet zur Speicherung der Informationen über die Objekte eine Datenbank.

Einsicht und Rechte auf die Datenbank des AD haben nur die Administratoren der HZD und die entsprechenden Administratoren des Fachgebietes „Informationstechnik“.

2.2 Netzwerk

Die Mitarbeiter des LLH arbeiten im Netz des Landes Hessen „ITSHESSEN“. Der Zugang zum Netz und der damit verbundene Zugriff auf die entsprechenden Dienste, Anwendungen und Datenstrukturen wird durch die Administratoren aus dem Fachgebiet „Informationstechnik“ eingerichtet. Es düfen nur entsprechend konfigurierte Systeme im Netz des Landes Hessen betrieben werden.

2.3 Serversysteme

Um die notwendigen Anwendungen und Dienste zur Verfügung zu stellen, sind entsprechende Serversysteme im Einsatz, die durch die Mitarbeiter des Fachgebietes „Informationstechnik“ oder durch die HZD verwaltet und betreut werden. Die Benutzer haben nur Zugriff im Rahmen ihrer Aufgaben auf die Serversysteme.

2.4 Benutzersysteme

Für die tägliche Arbeit werden den Mitarbeitern des LLH Systeme zur Verfügung gestellt. Die Verwaltung der Benutzersysteme obliegt dem Fachgebiet „Informationstechnik“. Dazu sind entsprechende Administrationsberechtigungen auf den lokalen Geräten und über die Domäne eingerichtet. Die Administration darf nur von den berechtigten Personen aus dem Fachgebiet „Informationstechnik“ vorgenommen werden. Der Benutzer selber hat keine Administrationsrechte auf den Benutzersystemen.

Die Handhabung der Benutzersysteme ist in einem gesonderten Dokument „Dienstanweisung für den Einsatz von Arbeitsplatzcomputern (Benutzer-Dienstanweisung)“ beschrieben.

2.5 Ablagestruktur

Daten können in verschiedenen Verzeichnissen auf dem lokalen Laufwerk (soweit vorhanden) oder den Netzlaufwerken abgelegt werden. Grundsätzlich sollen dienstliche Daten nur auf den Netzlaufwerken gespeichert werden, da für die lokalen Laufwerke keine Datensicherung erfolgt.

Folgende Laufwerke sind standardmäßig eingerichtet:

- Netzlaufwerke
  - J:\ -> Eigene Daten
  - P:\ -> Zentrale Datenablage (ZDA)
- Zusätzlich bei Arbeitsplatzrechnern und Notebooks:
  - D:\ -> Lokaler Datenträger
  - E:\ -> Geräte mit Wechselmedien (optional)
  - F:\ -> CD-Laufwerk oder DVD-Laufwerk (optional)

Das Netzlaufwerk (**P**) dient ausschließlich der Ablage dienstlicher Dateien. Hier sind die jeweiligen bereichsinternen Verzeichnisse und ein bereichsübergreifendes Verzeichnis in der jeweils abgesprochenen Struktur angelegt.

Für die Verwaltung der Ablagestruktur werden Administrationsrechte benötigt. Durch die Rolle der Administration ist eine Einsicht in alle Bereiche der Ablagestruktur möglich. Eine individuelle Verschlüsselung der Dateien ist möglich; diese Dateien können auch von dem Administratoren nicht mehr eingesehen werden.

Die Sicherung der auf den Netzlaufwerken (J) und (P) abgelegten Daten wird täglich zentral von der HZD vorgenommen. Daten auf dem lokalen Laufwerk (D), zu denen auch der Ordner "Eigene Dateien" gehört, werden nicht gesichert. Hier ist jeder Benutzer in der Verantwortung.

2.6 Passwortverfahren

Aus Gründen des Datenschutzes und der Datensicherheit sind die Computer oder Benutzerkonten nur durch die Eingabe eines Kennwortes zugänglich.

- Das Passwort wird von dem Benutzer bestimmt und muss spätestens nach 30 Tagen geändert werden.
- Ein einmal verwendetes Passwort darf erst nach 13 Zyklen wieder verwendet werden.
- Es muss mindestens aus 8 und darf höchstens aus 14 Zeichen bestehen.
- Nach 5 Fehlversuchen bei der Passworteingabe ist das Benutzerkonto zu sperren.
- Die Entsperrung des Kontos erfolgt nach Anweisung des betroffenen Benutzers durch die Administratoren oder automatisch nach frühestens 30 Minuten.
- Das Passwort kann bei Bedarf durch die Administratoren zurückgesetzt werden.

Voreingestellte Passwörter des Herstellers sind sofort zu ändern.

Vorläufige Passwörter sind durch den Benutzer nach der 1. Anmeldung zu ändern.

Der Administrator hat die Passwort-Regeln der IT-Benutzer technisch umzusetzen und deren Einhaltung technisch zu unterstützen.

2.7 Dokumentation

Die Zugriffsrechte sind von den Administratoren des Fachgebietes „Informationstechnik“ in Abstimmung mit der jeweils verantwortlichen Fachgebietsleitung einzurichten, zu dokumentieren und vor Manipulationen zu schützen.

3. Verwaltung der IT-Systeme

Soft- und Hardware sind durch die Administratoren so zu konfigurieren, dass ohne weiteres Zutun des Benutzers ein hoher Sicherheitsstandard im Rahmen der verfügbaren Möglichkeiten erreicht werden kann.

Die Nutzung aller nicht ausdrücklich erlaubten Dienste ist im Rahmen der verfügbaren Möglichkeiten zu unterdrücken. Dienste und Berechtigungen, die nicht oder nicht mehr benötigt werden, sind durch den Administrator zu deaktivieren.

3.1 Wartung

Der Administrator ist dafür verantwortlich, dass die Informationsverarbeitung möglichst störungsfrei abläuft. Hard- und Softwarekomponenten sind daher ordnungsgemäß zu warten. Die Wartungs- und Reparaturarbeiten sind – sofern möglich – außerhalb der normalen Bürozeiten durchzuführen, wenn diese zu Beeinträchtigungen des laufenden Betriebs führen können. Ansonsten sind die Benutzer vorab zu informieren.

Durch die Administratoren sind regelmäßig sicherheitsrelevante Patches, Updates oder sonstige Hilfsmittel zur Behebung von Sicherheitslücken einzupflegen.

Die mit Änderung der Berechtigung verbundenen Maßnahmen sind nach Art, Inhalt und Zeitpunkt zu protokollieren.

Wird Hardware zu Wartungszwecken außer Haus gegeben, sind alle sensitiven Informationen, die sich auf Datenträgern befinden, vorher zu sichern und zu löschen. Die Übergabe bzw. der Transport ist sicher zu gestalten.

3.2 Fernwartung/Remoteunterstützung

Um auf räumlich entfernten Rechnersystemen Unterstützung im Fehlerfall leisten zu können oder Wartungsarbeiten durch zu führen, wird im LLH das im Betriebssystem integrierte Werkzeug der Remoteunterstützung eingesetzt. Mit dieser Technik kann der Administrator den entfernt stehenden Rechner "übernehmen" und die festgestellten Fehler beseitigen.

Der Einsatz dieser Technik erfolgt ausschließlich zur schnellen Fehleranalyse und -beseitigung und zur Wartung der IT-Systeme.

Die Remoteunterstützung erfolgt immer mit der Zustimmung des betroffenen Benutzers. Die "Übernahme" eines APC ohne Wissen und Wollen des Nutzers kommt keinesfalls in Betracht.

Während der Remoteunterstützung halten der Nutzer und der Administrator i.d.R. telefonischen Kontakt.

3.3 Dokumentation

Die IT-Systeme und das Netz sind ausführlich und für Dritte nachvollziebar zu dokumentieren.

Jegliche Änderungen und Anpassung (Installationen, Konfigurationsänderungen, Einbau/Ausbau von Hardware und Peripherie, Treiberinstallation u.ä.) sind verpflichtend zu dokumentieren und der Fachgebietsleitung zeitnah mitzuteilen.

3.4 Vertretungsregelung

Jeder Administrator hat eine/n Vertreter/in einzuweisen und laufend zu informieren. Dokumentationen sind so zu gestalten, dass der/die Vertreter/in mit ihrer Hilfe seine Aufgaben wahrnehmen kann.

Für den Vertretungsfall ist eine Notfallkennung für einen Administrator mit erweiterten Berechtigungen angelegt. Das Passwort für diese Notfallkennung ist versiegelt und verschlossen aufzubewahren und die Benutzung zu dokumentieren.

3.5 Protokollierung und Kontrolle der IT-Dienste

Es ist eine regelmäßige Kontrolle der Funktionalität der IT-Dienste, der IT-Sicherheit und der Einhaltung der Dienstanweisungen durchzuführen. Zu diesem Zweck sind Systemprotokolle im Einsatz.

Bei Auswertungen von Protokollen mit personenbezogenen Daten ist das Vier-Augen-Prinzip anzuwenden.

Jeder Datenverkehr zwischen dem lokalen Netz des LLH und dem Internet wird aus Gründen der Datensicherheit einer automatischen vollständigen Protokollierung unterzogen.

Es wird ausdrücklich darauf hingewiesen, dass aus den Protokolldaten die Benutzerkennung des berechtigten Nutzers hervorgeht. Die Protokolldaten dürfen von dem Administrator ausschließlich zur Sicherstellung des technischen Betriebes ausgewertet werden. Eine Weitergabe ist nur in anonymisierter Form zulässig. Die Protokolldaten dürfen nicht für Zwecke einer Verhaltens- oder Leistungskontrolle verwendet werden.

Der Administrator ist für eine technisch leistungsfähige, sichere und geschützte Internetnutzung verantwortlich. Sieht er den Betrieb, im Hinblick auf *Datenschutz* und die *Datensicherheit* als gefährdet an, kann er Auszüge aus den Protokolldaten in anonymisierter Form dem Datenschutzbeauftragten zur Prüfung übergeben. Dieser entscheidet, ob sich begründbare sicherheitstechnische oder rechtliche Gefährdungen durch das Surf-Verhalten der Nutzer ergeben haben, die als erheblicher Verstoß angesehen werden können. Nur zur Klärung des begründeten Verdachtes können die Protokolldaten (und damit auch die Identität des Nutzers) durch den Datenschutzbeauftragten in Anwesenheit eines Mitglieds des zuständigen Personalrates ausgewertet werden.

Alle Personen, die Kenntnis über Surfverhalten und aufgerufene Web-Inhalte der Nutzer erlangt haben, sind zum Stillschweigen hierrüber verpflichtet. Die Pflicht zur Meldung strafrechtlich relevanter Tatbestände bleibt hiervon unberührt.

Der Administrator darf E-Mails und deren Anhänge nur unter Einbeziehung der betreffenden Beschäftigten öffnen, wenn eine begründbare sicherheitstechnische Gefährdung vorliegt. Eine Überprüfung, ob die E-Mail dienstlichen oder privaten Charakter hat, steht ihm daher nicht zu. Der Administrator ist zum Stillschweigen über den Inhalt von E-Mails und das E-Mailverhalten der Nutzer verpflichtet.

Die Öffnung von E-Mail-Postfächern und Benutzerkonten wird durch die Anlage „Verfahrensbeschreibung zur Öffnung von E-Mail-Postfächern und Benuzterkonten“ verbindlich geregelt.

Grundsätzlich ist es dem Personalrat des LLH oder einer beauftragten Person und den Datenschutzbeauftragten erlaubt, stichprobenartig Einsicht in die Protokolle zu nehmen.

3.6 Sicherheitsmaßnahmen/Virenschutz

Alle Nachrichten im Mailverkehr werden einer automatischen Überprüfung auf bekannt schädliche Inhalte unterzogen. Risikoträchtige, bzw. unerwünschte Dateianhänge und Inhalte (z. B. Makros) werden dabei automatisch ausgefiltert. Die Größe einer E-mail ist technisch auf 10 MB begrenzt. Da trotz dieser Sicherungsmaßnahmen Dateianhänge mit Schadensfunktion den Empfänger erreichen können, ist ein umsichtiger Umgang mit unverlangt zugesandten oder verdächtigen Nachrichten durch den einzelnen Benutzer erforderlich.

3.7 Verhalten bei eingetretenen Störungen

Alle Fehler und Probleme, die IT-Dienste betreffen, sind vom Administrator zu protokollieren.

Der Administrator hat bei Verlust der Netz- oder Systemintegrität schnellstmöglich diese Störungen zu beseitigen. Die Ursachen dieser Störungen sind anhand der erstellten Protokolle zu analysieren und Verbesserungen zu erarbeiten. Dies ist zu dokumentieren.

3.8 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.

4. Salvatorische Klausel

Es gilt die aktuelle Richtlinie zur Nutzung von E-Mail und Internetdiensten in der Hessischen Landesverwaltung des Hessischen Ministerium des Innern und für Sport sowie weitere Regelungen innerhalb der Hessischen Landesverwaltung.

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.

5. Schlussbestimmungen

Eine aktuelle "Übersichtsliste Administration" ist beigefügt. Veränderungen werden jeweils in der LLH-Info bzw. dem LLH-Intranet bekannt gegeben.

Die Verpflichtungserklärung, die von allen Administratoren akzeptiert und unterschrieben werden muss, ist ebenfalls zur Information als Anlage beigefügt. Bei einer Änderung der genannten Vorschriften ist eine schriftliche Bestätigung der Kenntnisnahme und der damit verbundenen Verpflichtungen durch die Administratoren einzuholen.

Diese Dienstanweisung tritt am .....in Kraft.

Änderungen und Ergänzungen sind jederzeit möglich. Die Gremien sind rechtzeitig einzubeziehen.

Kassel, den .....

_____
(Direktor)

ANLAGE: „Übersichtsliste Administratoren“

Die im LLH eingesetzte Hard- und Software wird von folgenden Administratorenkonten verwaltet:

1) Administratorengruppe mit umfassenden Berechtigungen:

Nachname	**Vorname**	***Telefonnr. (0561)***	***E-Mail-Adresse***	***Admin-Kennung***
Max	*Notfall****	*--*	*--*	

***** *Diese Kennung ist nur für den Notfall eingerichtet und keinem Mitarbeiter direkt zugeordnet. Das Passwort für diese Notfallkennung wird versiegelt und verschlossen aufbewahrt.*

2) Administratorengruppe mit eingeschränkten Berechtigungen

a) "Vor-Ort-Betreuer" mit örtlichen/lokalen Berechtigungen:

Nachname	**Vorname**	***Telefonnr.***	***E-Mail-Adresse***	***Admin-Kennung***

b) "Auszubildende" mit örtlichen/lokalen Berechtigungen:

Nachname	**Vorname**	***Telefonnr.***	***E-Mail-Adresse***	***Admin-Kennung***

ANLAGE: „Verpflichtungserklärung Administrator“

Die Administratoren werden darauf verpflichtet, die bei der Nutzung der IT-Dienste anfallenden Benutzerdaten nicht zum Zweck der Leistungs- und Verhaltenskontrolle der Beschäftigten zu nutzen. Die Weitergabe von Informationen und jede Form personenbezogener Auswertung der Verbindungs- und Benutzerdaten über den zur Aufgabenerledigung erforderlichen Umfang hinaus ist unzulässig.

Eine unrechtmäßige Herausgabe der Daten auch auf Verlangen von Vorgesetzten ist unzulässig.

ADMINISTRATOR NAME:

V e r p f l i c h t u n g s e r k l ä r u n g

Der Unterzeichner bestätigt die Kenntnisnahme der vorstehenden Regelungen, verpflichtet sich zu deren Einhaltung und bestätigt den Erhalt eines Abdruckes.

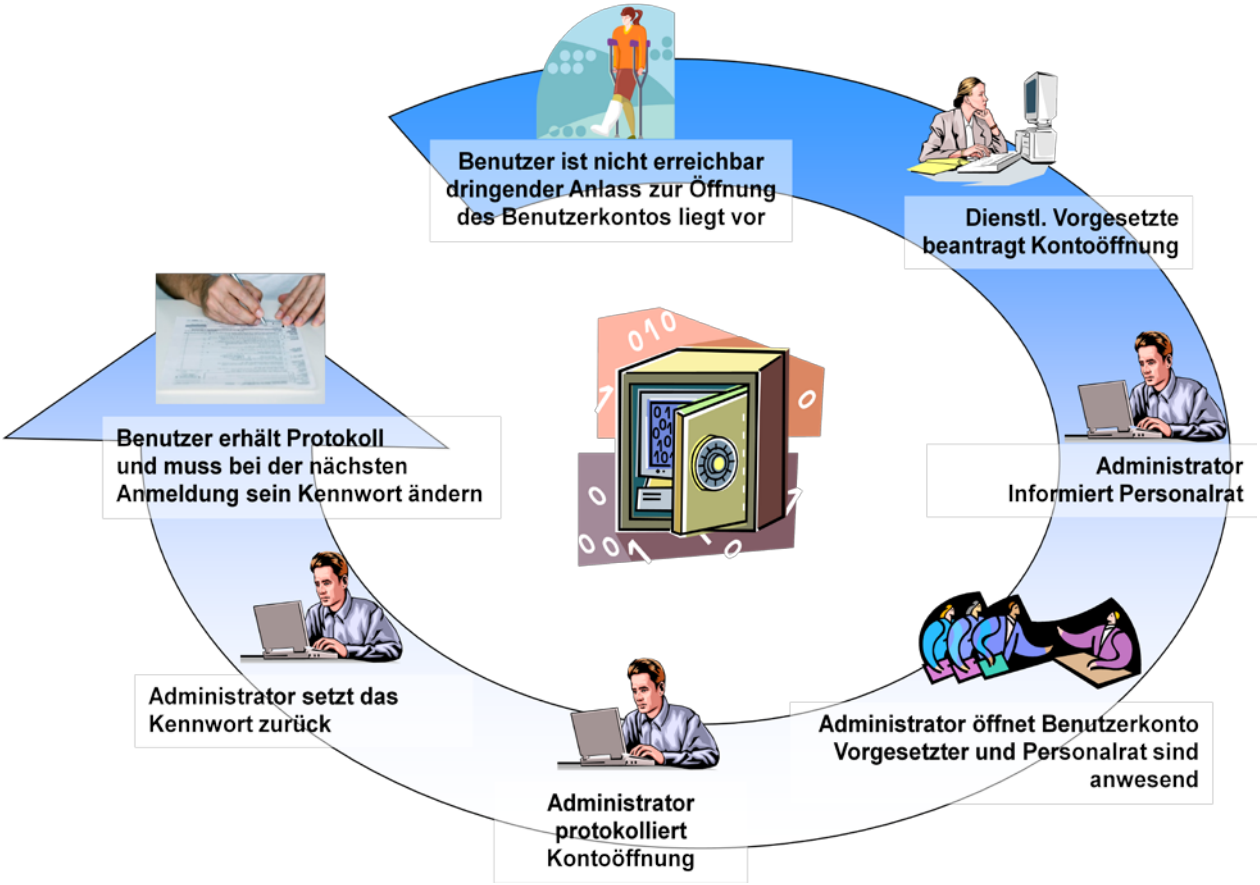
Dem Unterzeichner ist bewusst, dass Verstöße gegen die vorstehenden Regelungen arbeitsrechtliche Konsequenzen haben können.

Ort, Datum

_____
(Unterschrift Administrator)

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.

ANLAGE: „Zugriff auf Benutzerprofil“

Landesbetrieb Landwirtschaft Hessen

HESSEN

ZUGRIFF AUF BENUTZER PROFIL

Information an den Nutzer des Profils: _____

Wir Informieren Sie darüber das wir vom _____ bis _____ auf Ihr Profil zugegriffen haben.

Aus diesem Grund wurde Ihr Passwort geändert.

Ihre neues Passwort lautet: _____

Bitte ändern Sie das Passwort bei der nächsten Anmeldung!

Auftraggeber:		**Antragsdatum:**	
Grund der Nutzung:			
		_____ (Unterschrift Auftraggeber)	
Vom Personalrat zur Kenntnis genommen am:			
Name Personalratsmitglied:		_____ (Unterschrift)	
DURCHFÜHRUNG			
Profil geöffnet am:		**Uhrzeit:**	
Zusätzliche Bemerkungen:			
Ausführung unter Beobachtung/in Anwesenheit von:			
Name:	Unterschrift: _____		
Name:	Unterschrift: _____		
Name:	Unterschrift:		

Kompetenz für Landwirtschaft und Gartenbau LLH