Bundesministerium
des Innern

Bundesministerium des Innern, 11014 Berlin

Frau
Anna Biselli
[redacted]

Bundesministerium des Innern
Postausgangsstelle
25. März 2015
Anl.: [redacted]

HAUSANSCHRIFT
Alt-Moabit 101 D
10559 Berlin

POSTANSCHRIFT
11014 Berlin

TEL +49(0)30 18 681-1519
FAX +49(0)30 18 681-55038

ZI4@bmi.bund.de
www.bmi.bund.de

Betreff: Informationsfreiheitsgesetz
hier: IT-Sicherheitsrichtlinie (Hausanordnung)

Bezug: Ihr Antrag vom 24. Februar 2015
Aktenzeichen: ZI4-13002/4#531
Berlin, 24. März 2015

Anlage: - 1 -

Sehr geehrte Frau Biselli,

mit E-Mail vom 24. Februar 2015 beantragen Sie auf Grundlage des Informationsfreiheits-gesetzes (IFG) die Übersendung der IT-Sicherheitsrichtlinie (Hausanordnung Gruppe 3 Blatt 4.1des BMI).

In der Anlage erhalten sie das gewünschte Dokument. Ich hoffe, Ihnen hiermit weitergeholfen zu haben.

Mit freundlichen Grüßen
Im Auftrag
[redacted]
Menz

Hausanordnung

Einsatz von Informationstechnik (IT)[1]

Inhaltsverzeichnis

[1] Diese Hausanordnung ersetzt die Hausanordnung Gruppe 3 Blatt 4.1 „Richtlinie zum Einsatz von Informationstechnik im Bundesministerium des Innern" Version 1.4 (Stand: 25. Juni 2007) und die Hausanordnung Gruppe 3 Blatt 4.3 „Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz". Die „Dienstvereinbarung zwischen dem Bundesministerium des Innern und dem Personalrat im Bundesministerium des Innern über die Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz" (Stand: 7. August 2007) sowie die „Dienstvereinbarung zwischen dem Bundesbeauftragten für den Datenschutz und dem Personalrat im Bundesministerium des Innern über die Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz" (Stand: 22. April 2003) bleiben unberührt. Die maßgeblichen Regelungen wurden in diese Hausanordnung übernommen.

1 Allgemeines

1.1 Zweck und Geltungsbereich

Die Hausanordnung regelt den Umgang mit der Informationstechnik (IT) im BMI einschließlich BAköV und BfDI. Für die Mitarbeiter des BfDI gelten die Regelungen soweit sie die in dieser Hausanordnung aufgeführte Informationstechnik nutzen (z. B. i*net). Sie gilt nicht für IT, die zu Testzwecken durch die Abteilung Z betrieben wird. Sofern zu Zwecken der VS-Datenverarbeitung abweichende Regelungen bestehen bzw. getroffen werden, haben diese Vorrang gegenüber den hier festgelegten Bestimmungen.

1.2 Allgemeiner Vorrang der Nutzung elektronischer Verfahren

In den Arbeitsabläufen sind elektronische Verfahren soweit wie möglich zu nutzen (§ 12 Absatz 1 GGO).

1.3 Infrastrukturelle Voraussetzungen

Alle Liegenschaften des BMI sind über IT-Netzwerke in eine gemeinsame Kommunikationsinfrastruktur eingebunden. Zu diesen Netzwerken gehören der Informationsverbund Berlin Bonn (IVBB/Intranet des Bundes), der Informationsverbund für die Bundesverwaltung (IVBV) und weitere Netzwerke (z.B. DOI-Netz)[2]. Über diese Netzwerke erfolgt der Informationsaustausch mit

- angeschlossenen Stellen des Bundes,
- angeschlossen externen Stellen und
- externen Stellen außerhalb dieser Netzwerke über das Internet.

1.4 Benutzerservice

Der im Referat Z II 1 (Informations- und Kommunikationstechnik) verortete Benutzerservice unterstützt die Mitarbeiter des Hauses bei der Lösung technischer Probleme und berät bzw. betreut sie in allen informationstechnischen Angelegenheiten.

Die Kontaktaufnahme mit dem Benutzerservice kann zu den im i*net veröffentlichten Service-Zeiten telefonisch über die Durchwahl 1414, per E-Mail an Benutzerservice@bmi.bund.de (im globalen Adressbuch Benutzerservice (1414)) oder über das Programm HelpLine erfolgen, welches über Start > Hilfe und Support und einen Klick auf „Benutzerservice 1414“ aufrufbar ist.

[2] Zukünftig werden der IVBB und der IVBV durch die Netze des Bundes (NdB) abgelöst.

2 IT-Ausstattung

2.1 Standardausstattung

Zur Hardware-Standardausstattung gehören Arbeitsplatz-PC (APC), Bildschirm, Tastatur, Maus und Arbeitsplatzdrucker; zur Software-Standardausstattung die Ausstattung mit einem Betriebssystem und den damit verbundenen Programmen sowie einem Standard-Softwarepaket für die Erledigung fachlicher Aufgaben (Textverarbeitungs-, E-Mail- und Kalender-, Tabellenkalkulations- und Präsentationsprogramm).

2.2 Sonderausstattung

Zur Hardware-Sonderausstattung zählen insbesondere Laptop, Dockingstation, Mobiler digitaler Assistent (MDA), DVD-Laufwerk, Farbdrucker, Lautsprecher, Scanner, Mikrofone zur Spracherkennung, Beamer, Mobiltelefone (inklusive gesondert gesicherter Mobiltelefone (sog. Kryptohandys) oder SiMKo2).
Zur Software-Sonderausstattung gehört individuell entwickelte Software, die zur Erledigung von Fachaufgaben dient („Fachanwendungen"), sowie alle übrige Software wie z. B. Free- und Shareware. Die eigenhändige Installation von Software ist unzulässig.

Sonderausstattung wird nur bei einer Vereinbarkeit (Kompatibilität, Administrierbarkeit) mit der im Einsatz befindlichen Hard- und Software und bei einem angemessenen Kosten-Nutzen-Verhältnis auf schriftlichen Antrag des Anwenders und unter Verwendung des entsprechenden Formulars über den Benutzerservice bereitgestellt. Eine aussagekräftige Beschreibung der erforderlichen Funktionen und eine Begründung der dienstlichen Notwendigkeit mit Angabe von erwartetem Nutzungsumfang und -dauer sind daher erforderlich. Gefährdungen der IT-Sicherheit sind auszuschließen.

Bei einem Wechsel des Arbeitsgebietes, bei längerfristiger Abwesenheit (Abordnung, Beurlaubung etc.) und beim Ausscheiden aus dem BMI ist Sonderausstattung zurückzugeben bzw. wird Software-Sonderausstattung vom APC deinstalliert. Bleibt die Notwendigkeit bei einem Arbeitsgebietswechsel auch im Rahmen der neuen Verwendung bestehen, so ist die Sonderausstattung erneut, möglichst vor dem Wechsel, zu beantragen.

2.3 Befristete Ausgabe von Hardware-Sonderausstattung durch den Benutzerservice

Zur nicht dauerhaften Verwendung kann Hardware-Sonderausstattung (z.B. Laptop, Beamer, digitale Fotokamera) zur Verfügung gestellt werden. Entsprechende Anträ-

ge sind unter Angabe des Umfangs und der Dauer der Nutzung an den Benutzerservice zu richten.

2.4 Inventarisierung der Hardware

Die ausgehändigte Hardware ist Eigentum des Bundes. Den Erhalt bestätigt jeder Mitarbeiter durch seine Unterschrift. Eine Weitergabe an andere Mitarbeiter ist nicht gestattet. Das Entfernen oder Umkleben von Barcode-Aufklebern ist unzulässig.

2.5 Entwicklung von Fachanwendungen

Beim Referat Z II 1 kann ein Antrag auf Entwicklung einer individuellen Software zur sachgerechten Erledigung von Fachaufgaben gestellt werden. Dem Antrag ist ein Anforderungsprofil mit einer Beschreibung der zu unterstützenden Aufgabe und den damit verbundenen Anforderungen beizufügen. Das Referat Z I 2 (Organisation) und das Referat Z II 1 sind bei der Erstellung behilflich.

Fachanwendungen dürfen grundsätzlich nur durch das Referat Z II 1 entwickelt werden; Ausnahmen, insbesondere Eigenentwicklungen, bedürfen seiner vorherigen Zustimmung.

2.6 Ausschluss der Nutzung privater IT-Ausstattung im Dienst

Für die Erledigung dienstlicher Aufgaben dürfen nur vom Referat Z II 1 zugelassene und vom Benutzerservice installierte Hardware- und Software-Komponenten verwendet werden. Die Einbringung und Nutzung privater Hard- und Software ist grundsätzlich unzulässig. Ausnahmen bedürfen der vorherigen Zustimmung des Referats Z II 1.

2.7 Nutzung von Hard- und Software, die für dienstliche Zwecke, jedoch nicht vom BMI, zur Verfügung gestellt wurde

Hard- und Software, die von anderen Behörden oder Institutionen (insb. der EU) zur Bearbeitung dienstlicher Angelegenheiten zur Verfügung gestellt wurde, muss vor deren Einsatz durch das Referat Z II 1 geprüft werden.

2.8 Nutzung der dienstlichen IT-Ausstattung

Die zur Verfügung gestellte IT-Ausstattung darf, soweit im Einzelfall nichts anderes bestimmt ist, nur für die Erfüllung dienstlicher Aufgaben eingesetzt werden.

3 Zugriffsrechte

3.1 Standardberechtigung

Mit der Zugangskennung (siehe Ziffer 4.1) sind Nutzungsrechte entsprechend dem IT-Rechte-Konzept des BMI verbunden. Es werden insbesondere Zugriffsrechte für

- das Intranet des BMI (i*net),
- das Intranet der Bundes (www.intranet.bund.de),
- das Internet nach erfolgter Einweisung,
- die Ablagen der Organisationseinheit (OE), wie Laufwerk(e) und E-Mail-Ablagen,
- das personenbezogene Laufwerk (Laufwerk P: bzw. Ordner „Eigene Dateien"),
- das Postfach der OE (Referatspostfach) und
- das personenbezogene Postfach

vergeben.

3.2 Besondere Zugriffsrechte

Darüber hinausgehende Zugriffsrechte, z.B. auf einzurichtende OE-übergreifende Sonder-Laufwerke, werden auf schriftlichen Antrag des Leitors der beantragenden OE an den Benutzerservice vergeben. Neben einer Begründung der dienstlichen Notwendigkeit sind Nutzungsumfang und -dauer anzugeben. Die besonderen Zugriffsrechte werden bei längerfristiger Abwesenheit, beim Wechsel des Arbeitsgebietes oder beim Ausscheiden aus dem BMI ohne gesonderten Hinweis entzogen. Bleibt die Notwendigkeit auch im Rahmen der neuen Verwendung bestehen, ist sie erneut, möglichst vor dem Wechsel, zu beantragen.

4 IT-Sicherheit

4.1 Zugangskennung

Zum Schutz der IT-Systeme vor unbefugter Nutzung und Missbrauch wird der individuelle Zugang nur nach vorheriger Eingabe der Zugangskennung (Benutzername mit dazugehörigem Passwort) gewährt.

Das Passwort muss eine Länge von mindestens sechs Zeichen haben und ist in regelmäßigen Zeitabständen auf Aufforderung des IT-Systems zu ändern. Das Passwort darf weder anderen Mitarbeitern noch sonstigen Personen zur Kenntnis gegeben werden. Mitarbeiter sind -- auch zur Erfüllung ihrer administrativen Aufgaben – nicht berechtigt, das Passwort des Nutzers zu erfragen.

4.2 Schutz des APC vor der Nutzung durch Unbefugte

Zum Schutz vor Nutzung durch Unbefugte ist der APC beim auch nur kurzfristigen Verlassen des Büros zu sperren. Die Sperrung erfolgt durch Aktivierung des Kennwortschutzes (Strg + Alt + Entf > Computer sperren oder Windows-Taste + L). Die Hausanordnung Gruppe 10 Blatt 1 Berlin/Bonn gilt entsprechend.

4.3 Umgang mit beweglichen Datenträgern

Bewegliche Datenträger sind alle transportablen Speichermedien wie z.B. Disketten, CD-Rom, DVD oder USB-Speichersticks.

4.3.1 Verwendung von CD-ROM-, DVD- und anderen Laufwerken sowie USB-Speichersticks

Die in den APC z.T. standardmäßig installierten CD-ROM- bzw. DVD-Laufwerke sind grundsätzlich außer Betrieb gesetzt. Die Freischaltung bzw. die Ausstattung mit einem solchen Laufwerk oder einem USB-Speicherstick erfolgt nur auf schriftlichen Antrag beim Benutzerservice unter Verwendung des entsprechenden Formulars. Voraussetzung ist eine zwingende dienstliche Notwendigkeit, die unter Angabe von Nutzungsumfang und -dauer zu begründen ist. Die zugehörigen beweglichen Datenträger sind, soweit nichts Besonderes bestimmt ist, verschlossen aufzubewahren.

4.3.2 Nutzung von Daten auf beweglichen Datenträgern

Soweit Daten, die sich auf beweglichen Datenträgern befinden, genutzt werden sollen, sind diese vorab vom Benutzerservice auf Viren oder andere Schadprogramme zu prüfen. Dieser stellt im Anschluss die Daten wahlweise auf dem personenbezogenen Laufwerk P: oder auf dem Laufwerk der OE (Laufwerk L:) zur Verfügung.

4.3.3 Transport von Daten

Zum Transport von dienstlichen Daten bzw. zur Übertragung dienstlicher Daten, auch sofern es sich um Daten Dritter handelt, in andere Systeme können über den Benutzerservice USB-Speichersticks beantragt werden. Diese besitzen einen biometrischen Zugangsschutz (Fingerabdruckscan) und werden bei der Ausgabe auf den Benutzer personalisiert. Die Geräte dürfen nicht zum Transport von VS-Daten, Personalaktendaten[3] oder „besonderer Arten" personenbezogener Daten[4] eingesetzt werden. Die Übertragung von Daten in das Netz des BMI erfolgt wie unter Ziffer 4.3.2 angegeben. Das Kopieren, der Transport und die Nutzung von nicht vom BMI autori-

[3] Personalaktendaten sind Unterlagen, die die Beschäftigten betreffen, soweit sie mit ihrem Dienstverhältnis in unmittelbarem Zusammenhang stehen, vgl. § 106 Abs. 1 BBG.

[4] „Besondere Arten" personenbezogener Daten sind z.B. gem. § 3 Abs. 9 BDSG Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

sierten ausführbaren Dateien (siehe Ziffer 6.2.9) ist unzulässig. Die Aufbewahrung hat wie unter Ziffer 4.3.1 angegeben zu erfolgen.

4.4 Umgang mit mobiler Informationstechnik

Mobile IT-Geräte (Laptop, MDA etc.) sind grundsätzlich verschlossen aufzubewahren. Ausgehändigte Schlüsselmittel (z.B. USB-Token für Laptops) sind hiervon getrennt verschlossen aufzubewahren.

Bei Verlust eines mobilen IT-Geräts ist unverzüglich der Benutzerservice zu informieren. Außerhalb der Servicezeiten ist das Referat Z II 1 über das Lagezentrum zu informieren. Bei einem Diebstahl ist zusätzlich Anzeige bei einer Polizeidienststelle zu erstatten. Sofern Schlüsselmittel (z.B. Zertifikate auf MDAs, USB-Token für Laptops) von dem Verlust (mit-)betroffen sind, ist das Zertifikat über die RA-Stellen (Registration Authorities) im Referat Z II 3 (Innerer Dienst; Bibliothek; Sicherheitsbeauftragter des BMI) oder durch den Nutzer selbst unter Verwendung des bei der Zertifikatsausstellung festgelegten Sperrkennworts gegenüber der Zertifizierungsstelle zu sperren.

Bei Verlust eines dienstlich zur Verfügung gestellten Mobiltelefons ist unmittelbar der Benutzerservice zu informieren. Außerhalb der Servicezeiten ist das Referat Z II 1 über das Lagezentrum zu informieren. Die notwendige Sperrung der SIM-Karte wird durch das Referat Z II 1 beim Mobilfunkprovider veranlasst.

Mobiltelefone verfügen systembedingt nur über schwache Sicherheitsmechanismen. Sensible Informationen, insbesondere VS-Daten, Personalaktendaten oder „besondere Arten" personenbezogener Daten (siehe Ziffer 4.3.3) dürfen grundsätzlich weder auf dem Gerät selbst, noch auf einer damit verwendeten Erweiterungskarte (z.B. SD-Card) gespeichert oder - etwa per Kurznachrichten (SMS) - verarbeitet und versandt werden. Der Austausch von Daten mit einer Einstufung bis VS-NfD zwischen Kryptohandys (siehe Ziffer 2.2 und Ziffer 4.7) ist zulässig.

4.5 Änderungen bei Hard- und Software

Soweit Änderungen bei Hard- oder Software notwendig sind, werden die betroffenen Nutzer über den Benutzerservice oder auf andere geeignete Weise informiert. Stellt der Nutzer nicht angekündigte Änderungen an Hard- oder Software fest, so ist der Benutzerservice umgehend zu informieren.

4.6 Verhalten bei einer Warnung vor Schadsoftware

APC und Laptops sind durch zentrale Schutzvorrichtungen gegen den Befall durch Schadsoftware (Viren, Würmer, Trojanische Pferde u. ä.) geschützt. Zusätzlich wird eine regelmäßige Überprüfung der lokalen Festplatten der APC durchgeführt, die vom Nutzer nicht abgebrochen werden darf.

Ein Befall mit Schadsoftware wird automatisiert unter Nennung der APC-Nummer an das Referat Z II 1 gemeldet. Falls weitere Schritte zum Entfernen der Schadsoftware erforderlich sind, wird der Nutzer vom Benutzerservice informiert. Den Handlungsanweisungen des Benutzerservices ist Folge zu leisten.

Soweit Nutzer Warnungen vor Schadsoftware oder Hinweise von anderen Stellen als dem Benutzerservice erhalten, sind diese dem Benutzerservice zu melden. Eine Weiterleitung entsprechender Warnungen oder Hinweise mittels E-Mail an andere Stellen oder an Mitarbeiter außerhalb des Benutzerservice ist unzulässig.

4.7 Einsatz von VS-Technik

Die Verarbeitung, Speicherung und Übermittlung von Informationen des Geheimhaltungsgrades VS-Vertraulich oder höher ist nur auf den dafür besonders zugelassenen und gekennzeichneten Geräten erlaubt.

Die Verarbeitung, Speicherung und Übermittlung von Informationen des Geheimhaltungsgrades VS-NfD und nicht eingestufter Informationen ist innerhalb des BMI und des IVBB ohne zusätzliche Sicherheitsmaßnahmen zulässig. Bei der Kommunikation mit externen Stellen außerhalb des IVBB ist zu beachten, dass VS-NfD-Dokumente nur mit besonderen, vom BSI dafür zugelassenen Schutzmaßnahmen übermittelt werden dürfen. Der Benutzerservice berät bei Auswahl und Nutzung dieser Verfahren.

Bei der Kommunikation über mobile Geräte (z.B. Handy oder MDA) ist zu beachten, dass VS-NfD-eingestufte Daten nur mit hierfür speziell zugelassenen bzw. einsatzempfohlenen Geräten übermittelt werden dürfen (z.B. Kryptohandys oder SiMKo2). Der Benutzerservice berät bei Auswahl und Nutzung dieser Geräte.

5 Dokumentenerstellung und -management

5.1 Erstellung von elektronischen Dokumenten

Für die Erstellung von elektronischen Dokumenten (Vermerken, externen und internen Schreiben, Leitungsvorlagen, Protokollen, Sprechzetteln etc.) sind grundsätzlich die im Textverarbeitungsprogramm Word zur Verfügung stehenden Dokumentenvorlagen zu verwenden. Werden andere Vorlagen benutzt, sind stets das vollständige Geschäftszeichen einschließlich der Angabe der zuständigen OE sowie Name und Telefonnummer des Bearbeiters anzugeben.

5.2 Behandlung von aktenrelevanten Inhalten

5.2.1 Ablage von aktenrelevanten Inhalten in der Dateiablage der OE

Aktenrelevante Dokumente und E-Mails, die sich in der Bearbeitung befinden, werden (ggf. inkl. Anlagen) in der Dateiablage Laufwerk L: der jeweiligen OE abgespeichert, sofern sie nicht bereits in die elektronische Akte übernommen wurden. Aktenrelevant sind alle Dokumente, die erforderlich sind, um Stand und Entwicklung der Vorgangsbearbeitung jederzeit aus den Akten vollständig nachvollziehen zu können. Eine Speicherung solcher Dokumente auf dem lokalen Laufwerk N: (Lokalbetrieb) ist nur für die Arbeit am Telearbeitsplatz oder in Ausnahmefällen (z.B. Ankündigung von Einschränkungen der IT aufgrund von Wartungsarbeiten) zeitlich befristet zulässig. Die Speicherung von Dateien auf dem Laufwerk C: ist unzulässig.

5.2.2 Einrichtung von Ordnern im Laufwerk

Für die Ablage elektronischer Dokumente sind durch die jeweilige OE aufgabenbezogene Ordner im Laufwerk einzurichten und fortlaufend zu pflegen. Zweckmäßig ist die Abbildung des Aktenplans im Verzeichnissystem. Die Ablage elektronischer Dokumente in personenbezogenen Ordnern, unnötige Doppelablage von Dokumenten und unverhältnismäßig lange Ordnernamen sind zu vermeiden. Dateien und Ordnernamen mit einer Länge von mehr als 256 Zeichen (Dateiname incl. Pfad) werden technisch nicht unterstützt.

5.2.3 Vergabe von Dateinamen

Zur Verbesserung der Suchmöglichkeiten ist folgende Systematik einzuhalten: Dateinamen beginnen grundsätzlich mit dem Erstellungsdatum (jeweils zweistellig: Jahr/Monat/Tag; Beispiel: "100601" für den 1. Juni 2010) und nehmen stichwortartig durch eine Kurzbezeichnung Bezug auf den Inhalt des Dokumentes. Datum und Kurzbezeichnung sowie einzelne Wörter der Kurzbezeichnung sollen durch einen Unterstrich getrennt werden (Beispiel: "100601_Zuwanderung_GE_V1" für Gesetzentwurf Version 1). Von der Vergabe von Sonderzeichen und zusätzlichen Punkten ist abzusehen.

5.2.4 Archivieren und Löschen

Die Dateiablage ist kein Archiv. Die Archivierung elektronischer Dokumente mit Aktenrelevanz erfolgt nach Ausdruck in der Akte; mit deren Einführung in der elektronischen Akte. Für die aktuelle Bearbeitung nicht mehr benötigte Dateien sind regelmäßig durch den zuständigen Bearbeiter aus der Dateiablage der OE zu löschen.

5.3 Löschen von Dokumenten mit personenbezogenen Daten

Elektronische Dokumente und E-Mails mit personenbezogenen Daten sind zu löschen, sobald sie für die dienstliche Aufgabenerfüllung nicht mehr erforderlich sind. Die Pflicht zur Archivierung elektronischer Dokumente mit Aktenrelevanz bleibt hiervon unberührt (siehe Ziffer 5.2.4). Besondere gesetzliche Löschfristen sind zu beachten.

5.4 Behandlung von nicht aktenrelevanten Inhalten

Dokumente und E-Mails mit nicht aktenrelevantem Inhalt sind regelmäßig zu löschen, wenn sie für die Aufgabenerfüllung nicht mehr erforderlich sind.

5.5 Ablage im personenbezogenen Laufwerk P:

Zur Speicherung von privatdienstlichen Inhalten steht das personenbezogene Laufwerk (Laufwerk P:) zur Verfügung. Durch Löschen nicht mehr benötigter Dateien ist das Speichervolumen so gering wie möglich zu halten. Wurden für die Aufgabenerfüllung notwendige Daten auf dem Laufwerk P: abgespeichert, so sind diese vor dem Wechsel des jeweiligen Mitarbeiters in eine andere OE bzw. beim Ausscheiden dem Nachfolger oder dem Leiter der OE durch Verlagerung in das Laufwerk L: zur Verfügung zu stellen.

Vor dem Ausscheiden aus dem BMI können privatdienstliche Dateien auf bewegliche Datenträger übertragen werden. Anträge sind unter Verwendung des entsprechenden Formulars an den Benutzerservice zu richten. Nach dem Ausscheiden wird die Benutzerkennung gelöscht.

Im Bedarfsfall kann das Referat Z II 1 nach entsprechender Vorankündigung eine statistische Nutzungsanalyse der Laufwerke P: durchführen, um hieraus Rückschlüsse auf die Notwendigkeit gezielter Optimierungsmaßnahmen zu ziehen.

5.6 Sicherung/Rücksicherung

Die auf der Dateiablage Laufwerk L: und dem personenbezogenen Laufwerk P: abgelegten Dateien werden (nachts) automatisch gesichert. Bearbeitungsstände des Vortages und ggf. auch vorangegangener Tage können auf diese Weise wiederhergestellt werden. Entsprechende Anfragen sind an den Benutzerservice zu richten. Eine Wiederherstellung von im personenbezogenen Postfach oder öffentlichen Ordnern abgelegten Dateien ist nur bedingt möglich. Nähere Auskünfte gibt der Benutzerservice. Die lokalen Laufwerke C: bzw. N: werden nicht gesichert.

5.7 Drucken/Papierverbrauch

Zum sparsamen Umgang mit Papier sind Dokumente möglichst am Bildschirm zu lesen. Werden Dokumente in größerer Stückzahl benötigt, sind diese nur einmal aus-

zudrucken und dann zu kopieren. Hierfür stehen auf jeder Etage Kopierer zur Verfügung. Bei Ablichtungen mit mehr als 100 Kopien ist das Copy-Center oder ggf. über das Referat Z II 3 eine Druckerei zu beauftragen. Im Copy-Center können bei Bedarf auch Folien, Farbausdrucke und Farbkopien erstellt werden. Ablichtungen für private Zwecke sind gegen Kostenerstattung möglich und in die an den Kopiergeräten ausgelegten „Listen für Privatkopien" einzutragen.

5.8 Sonderregelungen für Verschlusssachen

Für die Herstellung sowie die Vervielfältigung von Verschlusssachen ist die Hausanordnung Gruppe 10 Blatt 3 zu beachten.

6 Bürokommunikation

6.1 Kalender

Um eine gemeinsame Terminplanung zu ermöglichen, sind alle dienstlichen und die dienstliche Verfügbarkeit beeinflussenden Termine im personenbezogenen elektronischen Terminkalender (Outlook) einzutragen.

Die Organisation von Terminen (z.B. Einladungen zu Besprechungen) erfolgt elektronisch unter Nutzung der Besprechungsplanung. Terminverschiebungen sind den anderen Teilnehmern durch Aktualisierung unter Angabe des Grundes elektronisch mitzuteilen. Ausfallende Besprechungen sind elektronisch abzusagen.

Urlaubszeiten, Gleittage, Mehrarbeitsausgleich, Krankheitstage sowie sonstige private Abwesenheiten sind in dem zentral geführten und für alle Mitarbeiter einsehbaren Kalender der OE als „private Abwesenheit" mit Namensangabe, Fortbildungen, Lehrgänge, Dienstreisen und sonstige dienstliche Abwesenheiten als „dienstliche Abwesenheit" mit Namensangabe zu vermerken.

In sonstigen elektronisch geführten Kalendern können Termine und Veranstaltungen von übergreifendem Interesse bekannt gemacht werden. Personenbezogene Daten dürfen in diesen Kalendern nur insoweit gespeichert werden, als sie von unmittelbarer Relevanz für die Durchführung der jeweiligen Veranstaltung sind. Sofern keine dienstliche Notwendigkeit mehr besteht, sind diese personenbezogenen Daten zu löschen.

6.2 E-Mail

E-Mail ist „elektronische Post", die an Empfänger sowohl im BMI (intern) als auch außerhalb des BMI (extern) versandt werden kann.

Eine E-Mail ist grundsätzlich mit einem aussagefähigen Betreff und einem Geschäftszeichen zu versehen.

6.2.1 Eingang von E-Mails

Das personenbezogene Postfach ist täglich mehrfach auf neue Posteingänge zu überprüfen. Können E-Mails nicht innerhalb einer angemessenen Frist beantwortet werden, ist dem Absender eine Zwischenbenachrichtigung zu übersenden.

Bei elektronischer Weiterleitung sind Geschäftsgangvermerke anzubringen. Die Regelungen der §§ 13 und 18 GGO gelten entsprechend.

E-Mails, die nicht der fachlichen Zuständigkeit des Empfängers unterliegen (Irrläufer), sind unverzüglich an die zuständige Stelle weiterzuleiten. Der Absender ist darüber entsprechend zu unterrichten. Ist die fachlich zuständige Stelle nicht bekannt, ist die E-Mail an die Zentrale Nachrichtenverteilung (ZNV) zu schicken. Ist eine eingegangene Nachricht nicht lesbar, kann sie ebenfalls an die ZNV oder an den Benutzerservice weitergeleitet werden.

6.2.2 Versand von E-Mails mit Aktenrelevanz (siehe Ziffer 5.2)

E-Mails sind grundsätzlich mit dem Postfach der OE bzw. dem funktionsbezogenen Postfach als Absenderangabe zu versenden. Dies erfolgt durch Aktivierung des „Von-Feldes" mit der Voreinstellung „Neue Nachricht als".

Für die Adressierung der E-Mail stehen drei Möglichkeiten zur Verfügung:

- „An": Hiermit wird der Hauptempfänger der Mitteilung ausgewählt. Hierbei ist grundsätzlich das Postfach der adressierten OE anzuschreiben.
- „Cc" (Carbon Copy): Cc entspricht der nachrichtlichen Unterrichtung und dient vor allem der Beschleunigung des Informationsflusses durch Adressierung an eine OE oder an einen persönlichen Empfänger. Die Verwendung sollte auf das notwendige Maß beschränkt bleiben (z. B. bei Rundschreiben).
- „Bcc" (Blind Carbon Copy): Die Namen von Empfängern, die mit Bcc adressiert werden, sind für keinen anderen Empfänger dieser E-Mail sichtbar. Die Nutzung dieser Funktion kommt insbesondere beim Versand an externe Empfänger außerhalb der öffentlichen Verwaltung in Betracht.

Abzuschließen ist eine externe E-Mail mit einer einheitlichen Absenderkennung (E-Mail-Signatur) nach folgendem Muster:

Mit freundlichen Grüßen
im Auftrag
Vorname Nachname

Referat XY
Bundesministerium des Innern

Alt-Moabit 101 D, 10559 Berlin
Telefon: 030 18681-0000
Fax: 030 18681-0000 (des Referates) oder 03018-681-50000 (PC-Fax)
E-Mail: vorname.nachname@bmi.bund.de
Internet: www.bmi.bund.de

Bei einer internen E-Mail kann auf die Angaben „Bundesministerium des Innern", Adresse des BMI, E-Mail-Adresse und Internet-Adresse verzichtet werden. Bei Versendung über die Absender-Adresse der OE wird die Angabe einer E-Mail-Adresse empfohlen. Die Zeichnungsform nach der Grußformel und vor Vorname und Nachname hat bei einer internen E-Mail wie folgt zu erfolgen: Leiter der OE ohne Zusatz, nur der Abwesenheitsvertreter mit dem Zusatz „in Vertretung" und alle übrigen Angehörigen der OE mit dem Zusatz „im Auftrag".

Die Antwort auf eine E-Mail soll an diejenige OE erfolgen, deren E-Mail beantwortet wird; entsprechendes gilt bei funktionsbezogenen Angaben. Unter Cc kann derjenige Mitarbeiter aufgenommen werden, der für die absendende OE gezeichnet hat.

6.2.3 Behördenübergreifender E-Mail-Verkehr

Die unter Ziffer 6.2.2 dargestellten Regeln sind auch für den behördenübergreifenden E-Mail-Verkehr maßgeblich. Ist eine organisations- bzw. funktionsbezogene Adresse nicht eingerichtet oder bekannt, hat eine Übersendung an die E-Mail-Adresse der Poststelle des Adressaten zu erfolgen. Die Federführung in jedem angeschriebenen Ressort muss sich eindeutig, z.B. an der Nennung der jeweiligen federführenden OE eines Ressorts als Hauptadressat unter „An:", erkennen lassen.

Im Geschäftsverkehr nach außen ist die E-Mail-Adresse des jeweiligen OE-Postfachs anzugeben.

6.2.4 E-Mails mit VS-NfD-Inhalt

Dokumente, deren Inhalt als VS-NfD eingestuft ist, dürfen nur innerhalb des BMI oder des IVBB ohne zusätzliche Sicherungsmaßnahmen versandt werden. Die E-Mails sind im Betreff mit dem Hinweis „VS-NfD" zu versehen; der eingestufte Inhalt darf sich nicht im Text der E-Mail, sondern nur in einer Anlage befinden.

Das Übertragen bzw. Herunterladen von VS-NfD-eingestuften Dateianlagen auf MDAs ist nicht gestattet. Ausgenommen hiervon sind ausschließlich Geräte vom Typ SiMKo2. Bei Unsicherheiten zum zulässigen Adressatenkreis oder zum Einsatz einer entsprechend zugelassenen Verschlüsselungssoftware ist der Benutzerservice zu kontaktieren.

Zum Schutz der Vertraulichkeit des elektronischen Schriftverkehrs ist besonders bei der Kommunikation im Behördenumfeld der Einsatz der sogenannten Virtuellen Poststelle, die an zentraler Stelle die Ver- und Entschlüsselung des externen E-Mail-Verkehrs automatisiert vornehmen kann, zu empfehlen. Der Benutzerservice berät hierzu.

6.2.5 E-Mails in Personalangelegenheiten

E-Mails mit Inhalten die Personalangelegenheiten betreffen (z.B. Verträge, Personal- und Kabinettvorlagen), dürfen innerhalb des BMI sowie des IVBB nur zwischen personenbezogenen Postfächern ausgetauscht werden. Der Versand von E-Mails in Personalangelegenheiten sowohl aus als auch an Referats- bzw. Funktionspostfächer ist nicht zulässig. Für den Abwesenheitsfall ist die Vertretung sicherzustellen.

Sofern E-Mails in Personalangelegenheiten oder mit sensiblen persönlichen Informationen ausschließlich für den adressierten Empfänger innerhalb des BMI bestimmt sind, sind sie mit der Vertraulichkeitseinstellung „Privat" (im Menü „Optionen" unter „Verlauf/Nachrichtenoptionen") zu versenden; mit dieser Einstellung sind sie dem Postfach-Vertreter nicht zugänglich (siehe Ziffer 6.3.3).

6.2.6 Versand und Größenbeschränkung von E-Mails mit Anlagen

Um Probleme beim Versand einer E-Mail zu vermeiden, hat ihre Größe grundsätzlich 9 MB nicht zu übersteigen. Die Zahl der als Anlagen beigefügten Dokumente soll auf das notwendige Maß beschränkt werden und die Zahl fünf nicht übersteigen. Um den Adressaten eine Überprüfung zu ermöglichen, ist die Zahl der beigefügten Anlagen aufzuführen. Ist der Versand von mehr als fünf Dateien notwendig, sind diese vorab zu einer Datei zusammenzufassen. Bei Fragen steht der Benutzerservice zu Verfügung.

Um die Lesbarkeit beim Empfänger sicher zu stellen sowie aus Gründen der Datensicherheit sollen Anlagen grundsätzlich in einem Standard-Datenaustauschformat (PDF) versandt werden.

In den Fällen, in denen ein Versand der Anlagen im Standard-Datenaustauschformat nicht angezeigt ist (z.B. im Rahmen von Abstimmungsverfahren), ist dafür Sorge zu tragen, dass die betreffenden Anlagen (z.B. Dateien im MS-Word- oder MS-Excel-

Format) zuvor von allen Daten bereinigt wurden, die Rückschlüsse auf hausinterne Bearbeitungen sowie Beteiligungs- und Abstimmungsverfahren zulassen. Dies umfasst vor allem alle Änderungen, Anmerkungen oder Kommentare, die im Überarbeitungsmodus im Dokument eingefügt wurden.

6.2.7 Versand von E-Mails über zentrale oder eigene Verteiler

Grundsätzlich ist der Kreis der Adressaten einer E-Mail so eng wie möglich zu fassen. Ist dennoch die Versendung an einen größeren Adressatenkreis angezeigt, können die im Adressbuch des BMI vorhandenen Verteiler genutzt werden.

Eigene Verteiler können eigenverantwortlich und bedarfsgerecht im persönlichen Adressbuch oder über die Kategoriefunktion der Kontakte im eigenen Postfach und auch in den Referatsablagen eingerichtet werden.

6.2.8 Untersagung von Kettenbriefen

Als Kettenbriefe werden insbesondere E-Mails bezeichnet, die die Aufforderung enthalten, der Empfänger solle sie an eine Reihe weiterer Empfänger weiterleiten. Der Versand oder die Weiterleitung von Kettenbriefen ist untersagt.

6.2.9 Versand und Empfang ausführbarer Dateien

Ausführbare Dateien, insbesondere solche mit den Dateiendungen .exe, .pif, .com und .bat, dürfen nur mit ausdrücklicher Zustimmung (Autorisierung) des Referats Z II 1 versandt oder nach Empfang ausgeführt werden.

6.2.10 Größenbeschränkung des E-Mail-Postfachs

Zeichnet sich eine Überschreitung der Speicherkapazität des personenbezogenen Postfachs ab, erhält der Nutzer eine entsprechende Hinweismeldung. Nicht mehr benötigte Elemente sind zu löschen und weiterhin benötigte (aktenrelevante) Elemente in das Dateisystem (Laufwerk L:) zu verschieben. Bei Überschreitung der Speicherkapazität können keine E-Mails oder Besprechungsanfragen gesendet oder empfangen werden. Wird die Speicherkapazität im Fortgang weiterhin überschritten, kommt es zur vollständigen Sperrung des Postfachs. Nur der Nutzer selbst kann die Arbeitsfähigkeit durch Löschung entsprechender Elemente wiederherstellen.

6.2.11 E-Mail-Nutzung zu privaten Zwecken

Die E-Mail-Nutzung zu rein privaten Zwecken ist unzulässig.

6.2.12 Systemsicherheit

Das Referat Z II 1 betreibt automatisierte technische Anlagen, die der Erkennung von Dateien dienen, welche die IT-Sicherheit gefährden können. Im Verdachtsfall wird in

den Nachrichtenlauf eingegriffen. Betroffene Mitarbeiter werden über die ergriffenen Maßnahmen informiert.

6.3 Sonstige organisatorische Regelungen

6.3.1 Bewertung per E-Mail eingehender rechtlich bindender Erklärungen

Beim Eingang rechtsverbindlicher Erklärungen (z.B. Widersprüche), die der Schriftform bedürfen, per E-Mail ohne qualifizierte elektronische Signatur, sind die zuständigen Stellen verpflichtet, den Absender unter Bezug auf die E-Mail schriftlich und vorab elektronisch auf den Formmangel hinzuweisen.

Eingehende E-Mails, die Verwaltungsverfahren betreffen, für welche ein Schriftformerfordernis vorgeschrieben ist, sind hinsichtlich ihres Eingangszeitpunktes zu registrieren.

6.3.2 Abwesenheitsassistent

Sofern an Arbeitstagen eine mehr als 24-stündige Abwesenheit vom Dienst vorgesehen ist, ist der Abwesenheitsassistent mit Hinweis auf die Dauer der Abwesenheit zu aktivieren. Ferner ist ein Vertreter mit seinen Erreichbarkeitsdaten zu benennen und Hinweise auf eine erforderliche nochmalige Zuleitung an das jeweilige Referatspostfach zu geben.

Aus Sicherheitsgründen werden automatische Antworten des Abwesenheitsassistenten nicht an Empfänger außerhalb des IVBB[5] versandt.

6.3.3 Vertretungsregelungen

Für den Fall ihrer Abwesenheit haben die Mitarbeiter sicherzustellen, dass neu eingehende E-Mails auch den jeweiligen Vertreter erreichen. Den Vertretern ist lesender Zugriff auf den E-Mail-Posteingang einzuräumen, damit auch bei unvorhergesehenen Abwesenheiten eine fristgerechte Bearbeitung der Eingänge gewährleistet werden kann.

Ein Zugriff auf das Postfach durch den Vertreter ist ausgeschlossen, wenn der Absender die Vertraulichkeitseinstellung „Privat" (im Menü „Optionen" unter „Verlauf/Nachrichtenoptionen") aktiviert hat (siehe Ziffer 6.2.5).

E-Mails aus Workflow-Systemen, die personenbezogen arbeiten (z.B. TMS, eAZM, Urlaubsworkflow) und E-Mails der Laufbahnbetreuer des Personalreferats in konkreten Personalangelegenheiten werden mit der Vertraulichkeitseinstellung „Privat" versandt.

[5] Zukünftig werden der IVBB und der IVBV durch die Netze des Bundes (NdB) abgelöst.

6.3.4 Benachrichtigung von Kommunikationspartnern bei Zuständigkeitswechseln

Bei einem Wechsel von Zuständigkeiten sind BMI-interne und insbesondere externe Kommunikationspartner unter Nennung des Nachfolgers frühzeitig zu informieren.

6.3.5 IT-Ansprechpartner

Die jeweilige Leitung benennt für die OE einen IT-Ansprechpartner, der partielle Administrations- und Beratungsfunktionen innerhalb der OE übernimmt. Näheres wird jeweils in Abstimmung mit dem Referat Z II 1 vereinbart (siehe Ziffer 6.4.2).

6.4 Postfach der OE (Referatspostfach)

Für jede OE wird ein Postfach zum Empfang von E-Mails eingerichtet.

6.4.1 Eingangsbearbeitung

Eingangsempfänger für an das Referatspostfach übermittelte E-Mails ist der Leiter der OE. Dieser kann einen Mitarbeiter der OE mit der Eingangsbearbeitung beauftragen.

Das Referatspostfach ist täglich mehrfach auf neue Posteingänge zu überprüfen. Eingänge werden elektronisch und mit entsprechendem Geschäftsgangvermerk an den zuständigen Bearbeiter weitergeleitet. Posteingänge, die älter als sieben Tage sind, werden automatisch durch das E-Mail-System gelöscht.

6.4.2 Zugriffsberechtigungen

Grundsätzlich haben alle Mitglieder einer OE lesenden Zugriff auf das Referatspostfach. Die Zugriffsrechte werden vom IT-Ansprechpartner der OE verwaltet (siehe Ziffer 6.3.5).

6.5 E-Mail-Eingänge ohne definierten Empfänger und Prüfung von E-Mail-Eingängen auf Lage- und Berichtsrelevanz

E-Mail-Eingänge ohne definierten Empfänger werden dem Lagezentrum (Zentraler Posteingang) zugeleitet. Es bewertet den Eingang und leitet ihn an die fachlich zuständige OE weiter. Diese unterrichtet im Anschluss das Lagezentrum zu den eingeleiteten Maßnahmen, wenn ein Bezug zur Inneren Sicherheit besteht oder wenn davon ausgegangen werden muss, dass Maßnahmen außerhalb der Dienstzeit durch das Lagezentrum zu veranlassen sein könnten. Das Lagezentrum prüft solche Eingänge im Rahmen seiner Fachaufgabe zusätzlich auf „Lage- und Berichtsrelevanz".

E-Mail-Eingänge mit definiertem Empfänger, die einen Bezug zur Inneren Sicherheit haben, werden dem Lagezentrum in elektronischer Kopie zugeleitet. Es bewertet die Eingänge im Rahmen seiner Fachaufgabe auf „Lage- und Berichtsrelevanz". Die

fachlich zuständige OE unterrichtet das Lagezentrum zu eingeleiteten Maßnahmen, wenn davon ausgegangen werden muss, dass Maßnahmen außerhalb der Dienstzeit durch das Lagezentrum zu veranlassen sein könnten.

An Arbeitstagen in der Zeit zwischen 16:30 und 08:30 Uhr (freitags ab 14:30 Uhr) sowie an Wochenenden und an Feiertagen werden alle an Referats- bzw. Funktionspostfächer gerichteten Eingänge dem Lagezentrum in elektronischer Kopie zugeleitet. Dieses prüft die Eingänge (kursorische Prüfung) im Rahmen der Sicherstellung der ständigen Arbeitsbereitschaft des BMI zu einer notwendigen Vorabinformation des Eingangsempfängers sowie bei Bezug zur Inneren Sicherheit auf „Lage- und Berichtsrelevanz". Erforderliche Maßnahmen werden in Abstimmung mit der fachlich zuständigen OE eingeleitet und dokumentiert. Kann das Lagezentrum keine eindeutige Zuständigkeit/Zuordnung feststellen, leitet es den Eingang an das Organisationsreferat zur Klärung und Festlegung der Zuständigkeit weiter.

7 Intranet des BMI (i*net)

7.1 Zugangsberechtigung

Alle Mitarbeiter des Hauses und der BAköV haben Zugang zum i*net. Für die Mitarbeiter des BfDI gilt dies eingeschränkt (z.B. keine Nutzung des Zeiterfassungsworkflows).

Externe Personen erhalten lesenden Zugang zum i*net nach Maßgabe der ihnen übertragenen Aufgaben auf Antrag der fachlich zuständigen OE unter Beteiligung des Beauftragten für den Datenschutz im BMI. Der Antrag ist an den Benutzerservice zu richten.

7.2 Technische Systemadministration

Die technische Systemadministration des i*net wird durch das Referat Z II 1 wahrgenommen.

7.3 Workflows

Die im i*net eingerichteten Workflows sind zu nutzen.

7.4 Schulungen

Jeder Mitarbeiter hat die Möglichkeit der Teilnahme an einer Grundschulung zum Aufbau und Inhalt des i*net sowie zum Umgang mit dem Redaktionssystem. Den Abteilungsredaktionen werden vertiefte Schulungen zum Redaktionssystem angeboten.

7.5 Veröffentlichungen im i*net

Regelungen zur Veröffentlichung von Informationen im i*net trifft die Hausanordnung Gruppe 1 Blatt 3.

8 Intranet des Bundes

8.1 Zugangsberechtigung

Jedem Mitarbeiter steht der Zugang zum Intranet des Bundes offen (www.intranet.bund.de). Externe Personen erhalten den Zugang nach Maßgabe der ihnen übertragenen Aufgaben auf Antrag der fachlich zuständigen OE. Der Antrag ist an den Benutzerservice zu richten.

8.2 Einschränkungen in der Nutzbarkeit bestimmter Angebote

Aufgrund von Gefährdungen, die durch die Verwendung bestimmter Internet-Technologien entstehen, sind nicht alle Angebote im Intranet des Bundes in vollem Funktionsumfang nutzbar. Sollte die Nutzung derartiger Angebote aus dienstlichen Gründen notwendig sein, ist dies beim Benutzerservice zu beantragen.

9 Internet

9.1 Zugangsberechtigung

Der Zugang zum Internet wird in der Regel bei Annahme der dienstlichen Notwendigkeit gewährt. Vor Freischaltung des Internetzugangs hat der betreffende Mitarbeiter grundsätzlich an einer Sicherheitsschulung teilzunehmen. In Einzelfällen kann auf Antrag der OE-Leitung die Genehmigung zur Freischaltung vorab erteilt werden. Die Sicherheitsschulung ist in diesen Fällen zwingend zum nächsten durch das Personalreferat benannten Termin nachzuholen.

9.2 Nutzungsregeln

Unzulässig ist jede absichtliche oder wissentliche Nutzung des Internets, die gegen geltende Rechtsvorschriften und hausinterne Regelungen verstößt oder geeignet ist, den Interessen der Dienststelle oder deren Ansehen in der Öffentlichkeit zu schaden bzw. die Sicherheit des Behördennetzes zu beeinträchtigen. Dies gilt vor allem für

- das Verbreiten von Äußerungen, die den Eindruck erwecken könnten, sie geschehen im Namen des Dienstherrn,
- das Abrufen oder Verbreiten von Inhalten, die gegen persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen und

- das Abrufen oder Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, gewaltverherrlichenden oder pornografischen Äußerungen oder Abbildungen.

9.2.1 Herunterladen von Dateien (Download)

Das Herunterladen von Dateien, insbesondere von Dokumenten aus dem Internet, ist auf das aus dienstlicher Sicht zwingend notwendige Maß zu beschränken. Das Herunterladen von ausführbaren Dateien (Dateien mit den Endungen .exe, .bat, .com, .vbs, etc.) ist grundsätzlich untersagt. Soweit das Herunterladen solcher Dateien dienstlich notwendig ist, kann es durch den Benutzerservice erfolgen. Die eigenhändige Installation von Software ist ebenfalls untersagt.

9.2.2 Nutzbare Protokolle und Dienste

Die Nutzung des Internets ist auf WWW-Angebote (HTTP/HTTPS) beschränkt. Die Nutzung von anderen Diensten (FTP, News, Chat etc.) ist aus Gründen der IT-Sicherheit grundsätzlich nicht möglich. Werden WWW-Angebote in verschlüsselter Form (über HTTPS) genutzt, erfolgt zur Prüfung der übertragenen Daten auf einen eventuell enthaltenen Schadcode eine Entschlüsselung an den Firewall-Systemen des BMI (sog. SSL-Proxy). Der Übertragungsweg von den Firewall-Systemen bis zu dem APC wird anschließend erneut verschlüsselt. Die Untersuchung der Datenströme auf möglicherweise schädlichen Inhalt erfolgt, wie bei herkömmlichem HTTP-Verkehr, vollständig automatisiert; es werden hierüber keine zusätzlichen Protokolldateien angelegt.

9.2.3 Feststellung offensichtlich strafrechtlich relevanter Inhalte

Werden bei der Nutzung des Internets offensichtlich strafrechtlich relevante Inhalte festgestellt, sind diese unter Angabe der Internet-Adresse (URL) an den Benutzerservice zu melden.

9.2.4 Private Internetnutzung

Die private Nutzung in geringfügigem Umfang ist zulässig, soweit die dienstliche Aufgabenerfüllung und die Verfügbarkeit des IT-Systems für dienstliche Zwecke nicht beeinträchtigt werden sowie haushaltsrechtliche Grundsätze dem nicht entgegenstehen. Es gelten folgende Einschränkungen:

- Das Abrufen von kostenpflichtigen Informationen für den Privatgebrauch ist unzulässig.
- Im Rahmen der zulässigen privaten Nutzung von Internet und i*net dürfen keine kommerziellen oder sonstigen geschäftlichen Zwecke verfolgt werden.

9.3 Veröffentlichungen im Internet-Auftritt des BMI

Regelungen zur Veröffentlichung von Informationen im Rahmen des Internet-Auftritts des BMI trifft die Hausanordnung Gruppe 1 Blatt 3.

10 Protokollierung der IT-Nutzung

10.1 Protokollierte Daten

Von den durch E-Mail- und Internetnutzung anfallenden Verbindungsdaten werden Datum/Uhrzeit, Adressen von Absender und Empfänger und übertragene Datenmenge protokolliert.

10.2 Verwendungszweck der Protokolle

Die Protokolle nach Ziffer 10.1 werden ausschließlich zu Zwecken der Analyse und Korrektur technischer Fehler, der Gewährleistung der IT-Sicherheit, der Optimierung des Netzes, der statistischen Feststellung des Nutzungsgrades und der Auswertungen gemäß Ziffer 11 (Missbrauchskontrolle) verwendet.

10.3 Stichprobenartige Erhebung

Zur Überprüfung der Einhaltung der Regelungen dieser Hausanordnung können Mitarbeiter des Referats Z II 1 regelmäßige stichprobenartige Überprüfungen anhand der Protokolldateien durchführen. Die stichprobenartige Sichtung erfolgt hinsichtlich der aufgerufenen Websites nicht personenbezogen. Ergänzend kann eine Übersicht über das Volumen des ein- und ausgehenden Datenverkehrs erstellt werden. Ergeben sich hierbei Anhaltspunkte auf Verstöße gegen die Nutzungsregeln nach Ziffer 9.2, so geschieht die weitere Auswertung unter Einbeziehung des Beauftragten für den Datenschutz im BMI und des Personalrates des BMI.

10.4 Nutzung personenbezogener Daten

Die bei der Nutzung der elektronischen Kommunikationsdienste anfallenden personenbezogenen Daten werden nicht zur Leistungs- und Verhaltenskontrolle verwendet. Sie unterliegen der Zweckbindung nach Ziffer 10.2 und den einschlägigen datenschutzrechtlichen Vorschriften.

10.5 Löschung der im Rahmen der Internetnutzung anfallenden Protokolldaten

Die im Rahmen der Internetnutzung anfallenden Protokolldaten werden – sofern sie Personenbezug haben oder die Herstellung eines solchen ermöglichen – nach spätestens sechs Monaten gelöscht. Die Frist beginnt mit dem Tag der Protokollierung.

10.6 Löschung der im Rahmen der E-Mail- und PC-Fax-Kommunikation anfallenden Protokolldaten

Die im Rahmen der E-Mail- und PC-Fax-Kommunikation anfallenden Protokolldaten werden auf allen Mail- und Faxservern nach 90 Tagen gelöscht.

11 Maßnahmen bei Verstößen/Missbrauchsregelung

11.1 Prüfung bei Missbrauchsverdacht

Bei Verdacht auf missbräuchliche oder unerlaubte Nutzung des Internetzugangs gemäß dieser Hausanordnung aufgrund stichprobenartigen Kontrollen (siehe Ziffer 10.3), erfolgt eine Überprüfung durch eine durch die Abteilungsleitung Z eingesetzte Untersuchungsgruppe, der mindestens ein beauftragter Mitarbeiter des Referats Z II 1 und der Beauftragte für den Datenschutz im BMI angehören. Die Untersuchungsgruppe veranlasst gegebenenfalls weitere Untersuchungsmaßnahmen. Auf der Basis dieser erstellt sie einen Bericht an die Abteilungsleitung Z, der auch dem Betroffenen ausgehändigt wird. Der Betroffene ist anschließend zu hören.

11.2 Maßnahmen bei nicht geringfügiger Nutzung des Internetzugangs

Ist aufgrund der stichprobenartig durchgeführten Kontrollen (siehe Ziffer 10.3) oder der statistischen Auswertung der Übersicht des Datenverkehrs eine Häufung von offensichtlich nicht geringfügiger privater Nutzung des Internetzugangs zu erkennen, so werden – nach Information des betroffenen Beschäftigten – die nicht personenbezogenen Stichproben in einem Zeitraum von zwei Wochen weiterhin durchgeführt. Ergeben diese Stichproben oder die Auswertung des Datenvolumens keine Änderung im Nutzungsverhalten, so werden – wiederum nach Information des betroffenen Beschäftigten – die Protokolle der folgenden zwei Wochen durch die Untersuchungsgruppe nach Ziffer 11.1 personenbezogen ausgewertet. Die Abteilungsleitung Z ist über das Ergebnis zu informieren. Im Falle einer nachgewiesenen missbräuchlichen Nutzung wird gemäß Ziffer 11.1 und Ziffer 11.3 vorgegangen.

11.3 Dienstliche und rechtliche Konsequenzen bei Verstößen

Es gelten die Regelungen des Disziplinar- und des Tarifrechts. Ein Verstoß gegen die Regelungen dieser Hausanordnung zur Nutzung des Internets kann neben den dienst- und arbeitsrechtlichen Folgen auch strafrechtliche Konsequenzen haben.

Die Abteilungsleitung Z kann bei Verstößen gegen die Regelungen zur Nutzung des Internets die private Nutzung des Internetzugangs im Einzelfall untersagen bzw. das Recht zur Nutzung des Internets und seiner Dienste entziehen.

12 IT-Schulungen

IT-Schulungen werden durch AG Z I 1 (Personalangelegenheiten im BMI) oder durch von ihr Beauftragte durchgeführt. Eine Übersicht zu den Schulungen wird im i*net veröffentlicht. Die Teilnahme erfolgt je nach Schulungsbedarf auf Antrag, der auf dem Dienstweg AG Z I 1 zuzuleiten ist. Jeder Kursteilnehmer erhält nach Beendigung des Kurses ein Teilnahmezertifikat; eine Kopie ist durch den Teilnehmer an AG Z I 1 zu senden, das diese zur Personalakte nimmt.

Entsteht zwischen der Schulung und der Möglichkeit zur Anwendung des Gelernten eine zu lange Zeitspanne oder liegen andere wichtige Gründe für eine Wiederholung der Schulung vor, kann eine erneute Teilnahme bei AG Z I 1 beantragt werden.