Standeskommissionsbeschluss über die Informatiknutzung

vom 18. Dezember 2012 (Stand 1. Januar 2019)

Die Standeskommission des Kantons Appenzell I.Rh.,

gestützt auf Art. 39 Abs. 1 der Personalverordnung (PeV) vom 30. November 1998, *

beschliesst:

I. Allgemeine Bestimmungen

Art. 1 Geltungsbereich

[1] Dieser Beschluss regelt die Informatiknutzung der kantonalen Mitarbeiter[1)] im Rahmen ihrer Anstellung.

[2] Der Beschluss gilt auch für das Gesundheitszentrum Appenzell. Die Aufgaben und Rechte des Departemensvorstehers gemäss diesem Beschluss nimmt der Spitaldirektor wahr. *

[3] In Körperschaften und Betrieben mit einem vertraglichen Nutzungsrecht für kantonale Informatikmittel sorgt die jeweilige Behörde oder Betriebsleitung dafür, dass bei der Nutzung durch ihre Behördenmitglieder oder Angestellten die inhaltlichen Vorgaben nach Kapitel II und III dieses Beschlusses erfüllt werden.

[4] Für Standeskommissionsmitglieder gilt Abs. 3 sinngemäss.

Art. 2 Informatiksicherheitsbeauftragter

[1] Die Standeskommission bestimmt einen Informatik-Sicherheitsbeauftragten und einen Stellvertreter für die kantonale Verwaltung. Im Einverständnis mit den am AINet angeschlossenen Körperschaften und Betrieben können sie auch für diese ihre Funktion ausüben.

[1)] Die Verwendung der männlichen Bezeichnung gilt sinngemäss für beide Geschlechter.

* vgl. Änderungstabelle am Schluss des Erlasses

II. Nutzung von Informatikmitteln

Art. 3 Informatikmittel

[1] Informatikmittel sind Geräte und Teile davon, die in der Bearbeitung, Speicherung oder Übermittlung von elektronischen Daten eingesetzt werden können.

[2] Als Informatikmittel gelten insbesondere:

1. Computer aller Art, einschliesslich Notebooks, digitale Assistenten und Smartphones;
2. Datenträger aller Art, beispielsweise Harddisks, Disketten oder USB-Sticks;
3. AINet, Internet und E-Maildienste;
4. Elektronische Daten und Programme.

Art. 4 Nutzungszweck

[1] Die Nutzung von Informatikmitteln dient geschäftlichen Zwecken.

[2] Die private Nutzung ist punktuell erlaubt. Sie darf weder die Leistung des Mitarbeiters noch die Informatikstruktur beeinträchtigen noch dem Arbeitgeber Zusatzaufwand bringen oder Sicherheitsrisiken bergen. Sie kann in begründeten Fällen eingegrenzt oder verboten werden.

Art. 5 Datenspeicherung

[1] Die Datenspeicherung auf Geräten, die am AINet angeschlossen sind, ist auf einem Serverlaufwerk des Kantons vorzunehmen.

[2] Private Daten sind in der Regel auf privaten Datenträgern, zum Beispiel auf einem dafür vorgesehenen USB-Stick, zu speichern.

[3] Die Speicherung von geschäftlichen Daten auf entfernten Systemen, beispielsweise in Clouds, ist nicht erlaubt.

Art. 6 Fremdprogramme und Fremdgeräte

[1] Programme und Geräte gelten als fremd, wenn sie nicht durch den Kanton zur Verfügung gestellt wurden oder vom Amt für Informatik (AFI) nicht ausdrücklich zugelassen sind.

[2] Es dürfen keine Fremdprogramme installiert oder Fremdgeräte angeschlossen werden, es sei denn, der geschäftliche Auftrag verlangt diese Verwendung.

[3] Vertrauliche Geschäftsdaten sind auf Fremdgeräten verschlüsselt abzulegen und dort sofort zu löschen, wenn sie nicht mehr gebraucht werden.

Art. 7 Sicherheit

[1] Die Mitarbeiter schützen die von ihnen verwendeten Informatikmittel gemäss dem Stand der Technik vor unberechtigtem Gebrauch, insbesondere durch

1. Sperren der Computer oder Abmelden vom System beim Verlassen des Arbeitsplatzes;
2. Geheimhaltung der persönlichen Passwörter;
3. sorgfältige Aufbewahrung und Überwachung mobiler Geräte.

[2] Virenverdächtige Programme, Dateien, E-Mails und Anhänge dürfen nicht geöffnet oder weitergeleitet werden und sind zu löschen. In Zweifelsfällen kann Rücksprache mit dem AFI genommen werden.

[3] Die Mitarbeiter informieren den Vorgesetzten bei sicherheitsrelevanten Risiken umgehend, beispielsweise nach einem Verlust eines mobilen Geräts.

Art. 8 Anschluss an Netzwerke

[1] Informatikmittel dürfen nicht gleichzeitig im AINet und in einem anderen Netzwerk, beispielsweise in einem öffentlichen, drahtlosen Netz, geöffnet sein.

Art. 9 Veränderungen und Kopien

[1] Veränderungen an den bereitgestellten Informatikmitteln, insbesondere an der Konfiguration von Hardware, an den Systemeinstellungen und an der Software, und das Umgehen oder Entfernen von Sicherheitsvorkehrungen sind nicht erlaubt.

[2] Das Kopieren von Programmen ist, unter Vorbehalt von Sicherungskopien durch das AFI, unzulässig.

Art. 10 Pflichten beim Austritt

[1] Bei einem Austritt aus dem Dienstverhältnis sind die zur Verfügung gestellten Informatikmittel aufgeräumt zurückzugeben.

[2] Private Daten und E-Mails sind zu löschen. Für berufliche Daten und E-Mails ist nach Anweisung des Vorgesetzten vorzugehen.

[3] Kommt der Austretende diesen Pflichten nicht nach, kann das AFI in Absprache mit dem Vorgesetzten die Informatikmittel räumen.

Art. 11 Ausnahmen und Nutzungsvorgaben

[1] Das AFI kann von Einschränkungen nach diesem Kapitel in begründeten Fällen und in Absprache mit dem Vorgesetzten Ausnahmen erlauben.

[2] Die Informatikstrategiekommission des Kantons kann für die Nutzung von Informatikmitteln und für den sicheren Umgang mit diesen Richtlinien erlassen.

III. Einschränkungen für Internet und E-Maildienste

Art. 12 Einschränkungen Internetnutzung

[1] Internetnutzungen und Zugriffe auf Websites sind untersagt, wenn sie die Arbeit beeinträchtigen, die Informatikstruktur belasten, mit Sicherheitsrisiken verbunden sind oder gegen das Recht oder die guten Sitten verstossen.

[2] Die Informatikstrategiekommission des Kantons legt die untersagten Nutzungen und Zugriffe im Rahmen dieser Bestimmung in einer Liste fest, die den Mitarbeitern in geeigneter Form mitzuteilen und zugänglich zu machen ist. Untersagte Nutzungen und Zugriffe können elektronisch gesperrt werden.

[3] Als untersagt gilt insbesondere der Zugriff auf Websites mit erotischem oder pornographischem Inhalt oder mit gewaltverherrlichendem, rassistischem, sexistischem oder extremistischem Inhalt.

Art. 13 Einschränkungen E-Maildienste

[1] Die automatische Weiterleitung von E-Mails an externe E-Mail-Adressen ist untersagt.

[2] Das AFI kann die Anzahl der Adressaten und die Grösse der Anhänge aus betrieblichen oder technischen Gründen beschränken.

Art. 14 Ausnahmen

[1] Der Departementsvorsteher kann von den Einschränkungen nach diesem Kapitel geschäftlich bedingte Ausnahmen erlauben.

IV. Internet- und Mailüberwachung

Art. 15 Aufzeichnung

[1] Das AFI ist berechtigt, die Verkehrsdaten der Internetzugriffe und des E-Mail-Verkehrs aufzuzeichnen.

[2] Im Falle von Internetzugriffen dürfen die Benutzernamen, die aufgerufenen Internetadressen, die Zeit und das Datum des Zugriffs sowie die Grösse der heruntergeladenen Dateien protokolliert werden.

[3] Im E-Mail-Verkehr dürfen Absender- und Empfängeradressen, Betreffzeile, Zeit und Datum der Übermittlung, Grösse der Mails und Bezeichnung sowie Grösse der Anhänge aufgezeichnet werden.

[4] Die Kontrolldaten werden unter Vorbehalt von Verdachtsfällen spätestens nach 12 Monaten gelöscht.

Art. 16 Melderecht

[1] Mitarbeiter, die Anzeichen für einen Verstoss gegen diesen Beschluss oder gegen eine strafrechtliche Norm wahrnehmen, sind berechtigt, dem Informatik-Sicherheitsbeauftragten Meldung zu erstatten.

[2] Das AFI und der Informatik-Sicherheitsbeauftragte sind berechtigt, die verantwortlichen Stellen über festgestellte Anzeichen zu informieren.

[3] Vorbehalten bleiben Strafanzeigen gemäss Art. 15 des Einführungsgesetzes zur Schweizerischen Strafprozessordnung (EG StPO).

Art. 17 Massnahmen bei Anzeichen für Verstösse

[1] Bei Anzeichen für Verstösse sind technische oder organisatorische Massnahmen zur Unterbindung weiterer Verstösse zu prüfen.

[2] Der Informatik-Sicherheitsbeauftragte kann bei Anzeichen für einen Verstoss eine personenbezogene Auswertung der Kontrolldaten durch das AFI anordnen.

[3] Der Informatik-Sicherheitsbeauftragte zeigt die Durchführung einer personenbezogenen Auswertung dem betroffenen Mitarbeiter und dem jeweiligen Departementsvorsteher an. Der Mitarbeiter darf Einsicht in die Daten und Resultate nehmen.

[4] Erhärtet sich der Verdacht aufgrund der Auswertung der greifbaren Daten nicht, ist die personenbezogene Auswertung abzubrechen. Die personenbezogenen Daten sind umgehend zu löschen. Der Informatik-Sicherheitsbeauftragte informiert den betroffenen Mitarbeiter und den jeweiligen Departementsvorsteher.

Art. 18 Verstösse

[1] Wird ein Verstoss festgestellt, informiert der Informatik-Sicherheitsbeauftragte die fehlbare Person, deren Vorgesetzten und den jeweiligen Departementsvorsteher.

[2] Personenbezogene Daten, die einen Verstoss dokumentieren, werden gesichert und im Personaldossier vermerkt.

Art. 19 Technische Probleme

[1] Der Informatik-Sicherheitsbeauftragte kann personenbezogene Auswertungen anordnen, soweit dies zur Ermittlung der Ursachen für technische Probleme oder zur Gewährleistung der Funktionsfähigkeit des Informatiksystems unerlässlich ist.

[2] Eine Anzeige an die betroffenen Personen ist nur notwendig, wenn Anzeichen bestehen, dass die Ursache für die technischen Probleme und die Gefährdung der Funktionsfähigkeit Verstösse gegen diesen Beschluss sind.

V. Schlussbestimmungen

Art. 20 Sanktionen

[1] Im Falle von Verstössen gegen diesen Beschluss drohen neben strafrechtlichen Konsequenzen personalrechtliche Massnahmen und Schadenersatzansprüche.

[2] Das AFI kann im Einvernehmen mit dem Vorgesetzten insbesondere

1. Informatikmittel entziehen oder die Nutzung einschränken;
2. den Internet- oder E-Mailzugang einschränken oder sperren;
3. Daten oder Programme blockieren oder löschen.

Art. 21 Ablösung bisherige Vorgaben

[1] Dieser Beschluss löst die bisherigen Vorgaben für Informatiknutzer ab, insbesondere die Richtlinien für Informatikbenutzerinnen und -benutzer.

Art. 22 Inkrafttreten

[1] Dieser Beschluss tritt auf den 1. August 2013 in Kraft.

Änderungstabelle – Nach Beschluss

Beschluss	Inkrafttreten	Element	Änderung	cGS Publikation
18.12.2012	18.12.2012	Erlass	Erstfassung	-
06.12.2016	01.01.2017	Ingress	geändert	-
18.12.2018	01.01.2019	Art. 1 Abs. 2	geändert	--

Änderungstabelle – Nach Artikel

Element	Beschluss	Inkrafttreten	Änderung	cGS Publikation
Erlass	18.12.2012	18.12.2012	Erstfassung	-
Ingress	06.12.2016	01.01.2017	geändert	-
Art. 1 Abs. 2	18.12.2018	01.01.2019	geändert	--