IT-Anwenderreglement

vom 18. Dezember 2007

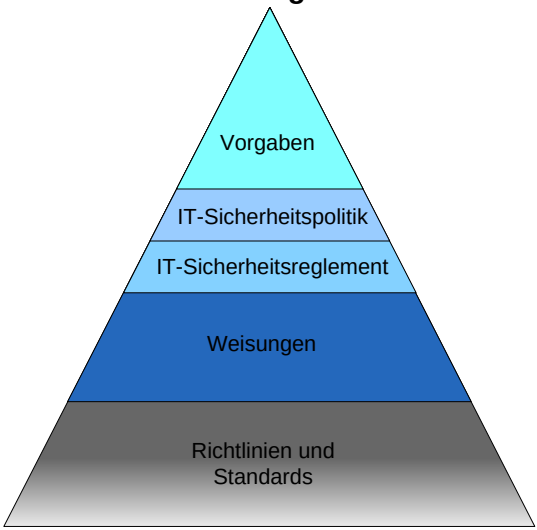
Der Stadtrat

in Koordination mit dem RRB vom 11. Dezember 2007

erlässt folgendes Reglement:

1. Einleitung

1.1 Vorbemerkungen



[1] Das IT-Anwenderreglement dient als Gesamtwerk über das Sicherheitsregelwerk der KSD (siehe Abb. 1). Weiter dient es als Bindeglied der in den einzelnen Schichten erarbeiteten Dokumente. Es stützt sich insbesondere auf folgende übergeordnete Rechtsgrundlagen und Dokumente ab:

ρ Personalgesetzgebung

- Datenschutzgesetzgebung

Diese Gesetze sind zu finden unter www.rechtsbuch.sh.ch für den Kanton, sowie unter www.rss.stadt-schaffhausen.ch für die Stadt.

- IT-Leitbild
- NSP (Network Security Policy)
- IT-Sicherheitspolitik
- IT-Sicherheitsreglement

*(siehe Intranet-Portal)**

** Im weiteren Verlauf wird mehrfach auf das Intranet-Portal verwiesen. Die angesprochenen Weisungen und Richtlinien sind im Intranet-Portal unter Informatikorgane, in der Rubrik IT-Grundschutz aufgeschaltet.*

[2] Die Umsetzung des vorliegenden IT-Anwenderreglements stützt sich auf den Regierungsratsbeschluss Nr. D/Sp/19/15 vom 9. Mai 2006 sowie den Stadtratsbeschluss Nr. 220 vom 23. Mai 2006 zur Umsetzung der IT-Sicherheitspolitik, des IT-Sicherheitsreglements und der zugehörigen Weisungen.

1.2 Geschlechtsneutrale Formulierung

Aus Gründen der einfacheren Lesbarkeit wird auf die geschlechtsspezifische Differenzierung, z.B. Anwender/-innen oder Benutzer/-innen verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für beide Geschlechter.

1.3 Abgrenzung

Dieses Dokument regelt den Umgang der Mitarbeitenden mit der Informatik. Es gilt als umfassendes Reglement für Kanton, Stadt und am SHNet angeschlossene Gemeinden.

1.4 Die wichtigsten Anforderungen aus Gesetzesartikeln

Persönlichkeitsschutz und Verhaltensüberwachung am Arbeitsplatz, Art. 26 Abs. 1 Verordnung 3 zum Arbeitsgesetz, ArGV 3, SR 822.113

Personalgesetz, SHR 180.100, RSS 311.1 Regelt die Rechten und Pflichten der Mitarbeitenden:

- Art. 18 Persönlichkeitsschutz
- Art. 34 Schweigepflicht
- Art. 30 Arbeits- und Treuepflicht
- Art. 36 Geistiges Eigentum

1.5 Kontrolle und Durchsetzung des Reglements

Bei der Kontrolle hat sich der Arbeitgeber an die Bestimmungen des Personal- und Datenschutzgesetzes zu halten. Er hat die Persönlichkeit der Mitarbeitenden (Privatsphäre am Arbeitsplatz) zu achten. Er ergreift angemessene organisatorische und technische Massnahmen, um dem vorliegenden Reglement und anderen Weisungen widersprechende Nutzungen der elektronischen Kommunikationsmittel zum vornherein auszuschliessen, z.B. durch Sperren bestimmter Webseiten, Einsatz von Antivirusprogrammen, Begrenzung des individuellen Speicherplatzes, etc. Unabhängig davon sind die Mitarbeitenden für die korrekte Nutzung verantwortlich.

1.5.1 Anonyme Auswertungen und Protokolle

Aus Gründen der Systemsicherheit werden laufend vollautomatisch und maschinell, d.h. ohne Kenntnisnahme durch eine Person, anonyme Überwachungen der technischen Ressourcen des SHNet in Form von Protokollierungen durchgeführt. Dabei kann die Einhaltung der vorliegenden Nutzungsregelung in anonymer Form überprüft werden. Eine personenbezogene Auswertung findet in der Regel nicht statt.

1.5.2 Personenbezogene Auswertung von Protokollierungen

Ergibt die anonyme Überprüfung oder andere Vorkommnisse Hinweise auf einen Missbrauch der elektronischen Kommunikationsmittel im Sinne einer widerrechtlichen oder weisungswidrigen Benutzung, kann eine personenbezogene Auswertung der Protokollierung folgendermassen vorgenommen werden:

- **Keine technische Störung**

Falls trotz Missbrauch keine technische Störung der Informatiksysteme vorliegt, informiert der Vorgesetzte den betroffenen Mitarbeitenden in einer speziellen schriftlichen Ankündigung, dass ab dem Zeitpunkt der schriftlichen Information während einer gewissen Zeit stichprobenweise eine personenbezogene Auswertung stattfinden wird. Diese Auswertung kann entweder durch den Vorgesetzten bei der KSD beantragt oder durch die KSD direkt initiiert werden.

- **Technische Störung**

Falls ein Missbrauch zugleich auch zu einer technischen Störung der Informatiksysteme geführt hat, wird die KSD zur Behebung dieser Störung ohne schriftliche Information an die betroffenen Mitarbeitenden eine personenbezogene Auswertung vornehmen. In die-

sem Fall können die involvierten Computerstationen sofort vom SHNet entfernt und die Vorgesetzten direkt informiert werden.

ρ **Art der Auswertung**

Grundsätzlich werden nur Bestandes- und Verbindungsdaten, jedoch nicht der Inhalt von E-Mails und/oder Webseiten, ausgewertet. In begründeten Fällen kann jedoch auch eine Auswertung des Inhalts stattfinden. Vorbehalten bleibt auch die rückwirkende Auswertung in schwerwiegenden Fällen. Zugriff auf die personenbezogenen Auswertungen haben der ISB (Informatik Sicherheitsbeauftragter) und die zuständigen Vorgesetzten. Eine Bekanntgabe an Drittpersonen findet grundsätzlich nicht statt. Eine personenbezogene Auswertung wird ausschliesslich für den entsprechenden Zweck, d.h. die Sanktionierung durch den Arbeitgeber bzw. die Behebung der technischen Störungen durch die KSD verwendet und anschliessend vernichtet.

1.6 Sanktionen bei Missachtung

Wenn ein Verstoss gegen personalrechtliche Pflichten, andere Bestimmungen (Gesetze, Erlasse, Verordnungen, Reglemente) oder das vorliegende Reglement festgestellt wird, kann abhängig vom Ausmass die Benutzerkennung (Benutzername und Passwort) blockiert, der Zugriff zum Netzwerk unterbunden oder der Internetzugang gesperrt werden. Dateien mit privatem Inhalt können von der KSD gegen Vorankündigung gelöscht werden. Vorbehalten bleiben straf- (StGB), zivil- (ZGB) und personalrechtliche (Personalgesetz Art. 41 und 42) Sanktionsmöglichkeiten. Ferner kann der Mitarbeitende für allfälligen Schäden des Arbeitgebers haftbar gemacht werden. Bei konkretem, begründetem Verdacht auf eine strafbare Handlung kann der Arbeitgeber Anzeige bei der zuständigen Behörde erstatten.

2. Verhalten bei IT-Störungen und IT-Notfällen

[1] Die KSD betreibt einen so genannten "single point of contact", an welchem eingehende Meldungen zentral erfasst und den entsprechenden Spezialisten umgehend weitergeleitet werden. Bei allen Anliegen kann davon ausgegangen werden, dass über diese zentrale Stelle am schnellsten und kompetentesten beraten wird.

Telefon: 052 632 77 88
E-Mail: helpdesk@ksd.ch

[2] Bei Vorliegen einer Störung wird persönlich oder via Telefonbeantworter informiert, welcher Art eine Störung ist und in welcher Frist sie behoben werden kann. Ein weiteres Medium zu Informationszwecken ist das Intranet. Aktuelle Störungen werden auch dort publiziert.
In Ausnahmefällen ist der Kommunikationsweg in der Weisung "Information im Ereignisfall" beschrieben (siehe Intranet-Portal).

[3] Im IT-Notfall oder -Katastrophenfall ist die KSD in einzelne Notfallteams gegliedert. Das Vorgehen der KSD respektive das Verhalten der IT in Krisensituationen ist in der Weisung "IT-Notfälle und –Katastrophen" geregelt. Dieses Dokument enthält weitere Anleitungen und Anweisungen (siehe Intranet-Portal).

3. Der Faktor Mensch

[1] Die IT-Sicherheit ist nicht allein durch technische Massnahmen zu erreichen. Sie bedingt auch ein sachgemässes Verhalten der Mitarbeitenden, sowie das Wahrnehmen von gewissen Verantwortungen. Neben dem externen Hacker kann auch der eigene Mitarbeitende dem Unternehmen schaden. Ein fehlerhaftes Verhalten kann grob in die folgenden Kategorien eingeteilt werden:

Beurteilungskriterien	Beispiele
Fahrlässigkeit	Versehentliches Löschen von Informationen
Grobfahrlässigkeit	Liegenlassen von ungeschützten elektronischen Datenträgern
Vorsatz	Schädigung der Unternehmung, Bereicherung des Mitarbeitenden, Vertrauliche Informationen veräussern oder löschen, etc.

[2] Durch den Einsatz technischer Schutzmassnahmen (Firewall, Spamfilter oder Antivirusprogramm) kann ein Teil der Gefahr gebannt werden.

3.1 Risiken der Datenverarbeitung

Der Bereich der Datenverarbeitung birgt weitere Risiken, wogegen technische Schutzmassnahmen nur bedingt entgegen wirken können. Der Mitarbeitende muss somit im Umgang mit Daten während

der Verarbeitung, der Speicherung und Kommunikation von Informationen entsprechend sensibilisiert agieren, so dass die Vertraulichkeit (nur Befugte haben "Zugang" zur Information bzw. können diese lesen) und die Integrität (Information ist unverändert seit der Erstellung) gewährleistet sind. Dadurch wird gleichzeitig die Verfügbarkeit der verwaltungsinternen Informationen sichergestellt.

Informationssicherheit	Mögliche Gefahren	Massnahmen
Vertraulichkeit der Daten	– Leichtfertige Preisgabe von vertraulichen Informationen durch die Mitarbeitenden – Unzureichender Zugangsschutz (Benutzer / System / Netzwerk)	– Berechtigungskonzept – Ablagekonzept – Verschlüsselung der Daten – Massnahmen gegen Spionage (z.B. abhören) / Hackerangriffe – Zutrittsregelungen
Integrität der Daten	– Technische Defekte, welche die Speicherung oder Datenübertragung verfälschen – Anwender kann Daten vorsätzlich oder fahrlässig verfälschen – Computerviren können Daten verändern	– Virenschutz – Verschlüsselungsverfahren (Signaturen) – Kompatibilitätsprüfung (Standards)
Verfügbarkeit der Daten	– Technische Störungen – Höhere Gewalt – Computerviren – Irrtümliches oder missbräuchliches Löschen benötigter Daten (Verlust) – Diebstahl oder Sabotage durch die Mitarbeitenden oder Dritte	– Datensicherung – Redundanz der Systeme (Ersatz-RZ, Raidsysteme, USV-Anlage, räumliche Trennung, …) – Archivierung – Notfallkonzepte

3.2 Awareness-Kampagnen

Um das Sicherheitsbewusstsein der Mitarbeitenden zu fördern und ihnen den sicheren Umgang mit Informatikmitteln zu erleichtern, wird die KSD regelmässig entsprechende Awareness-Kampagnen anbieten und durchführen. Mögliche Medien dazu sind: Broschüren, Infoveranstaltungen oder E-Learning. Nur durch die Hilfe der Mitarbeitenden kann die Informationssicherheit gewährleistet wer-

den und das aus IT-Sicht wichtigste Gut - die Daten - vor Gefahren geschützt werden.

3.3 Verantwortung und Konsequenzen

[1] Gleichzeitig wird von jedem Mitarbeitenden das Wahrnehmen von gewissen Verantwortungen vorausgesetzt:
Bei auftretenden Unregelmässigkeiten, z. B. unerklärlichem Systemverhalten, Verlust oder Veränderung von Daten und Programmen, Verdacht auf Missbrauch der eigenen Benutzerkennung (Benutzername und Passwort) oder ähnliches ist umgehend die KSD zu benachrichtigen. Es ist untersagt, eigene Versuche zu unternehmen, um die auftretenden Unregelmässigkeiten zu beheben.
[2] Die elektronischen Kommunikationsmittel dürfen von den Mitarbeitenden nur mit der gültigen persönlichen Zugangsberechtigung (Benutzername und Passwort) benutzt werden.
[3] Eingeschaltete Computerstationen müssen stets unter Aufsicht der Mitarbeitenden gehalten werden. Das Passwort darf weder anderen Personen mitgeteilt oder zugänglich gemacht werden, noch darf eine unberechtigte Person an eine im Betrieb stehende Computerstation zugelassen werden.
[4] In begründeten Fällen (wie z.B. Vertretung bei Abwesenheit) kann über die KSD der Zugriff auf die Daten eines Dritten mit der persönlichen (eigenen) Benutzerkennung (Benutzernamen und Passwort) eingerichtet werden. Stellvertretungen sind ausschliesslich über dieses Verfahren abzuhandeln.
[5] Neben den zentral gespeicherten Daten, unterliegen auch die lokal am Arbeitsplatz gespeicherten Daten einem grossen Gefahrenpotential. Die Mitarbeitenden sollten sich über ihr Verhalten am Arbeitsplatz bewusst sein. Sobald vertrauliche Informationen am Bildschirm angezeigt werden, sollte keine unberechtigte Person die Möglichkeit haben, diese einzusehen.
[6] Beim Verlust von IT-Geräten, die zum Eigentum der Verwaltung gehören, ist umgehend die KSD zu benachrichtigen. Diese Geräte werden für jegliche mit der Verwaltung in Verbindung stehende Kommunikationen gesperrt.
[7] Weitere Informationen zum Thema können in der Weisung "Sicherer Arbeitsplatz" eingesehen werden (siehe Intranet-Portal).

4. Umgang mit Informatikmitteln

4.1 Beschaffung

[1] Durch die im Regierungsratsbeschluss Nr. D/Sp/43/26 vom 23. November 2004 sowie dem Stadtratsbeschluss vom 23. November 2004 zur Umsetzung des Informatikleitbildes beschlossenen Beschaffungsrichtlinien, muss die Anschaffung von Informatikmitteln (Hardware und Software) über die KSD erfolgen. Neuerungen sind im Regierungsratsbeschluss Nr. 13/212 vom 3. April 2007 sowie dem Stadtratsbeschluss Nr. 186 vom 24. April 2007 zur Verabschiedung des von der KSD erstellten IT-Produktekataloges als Basis für die IT-Budgetierung 2008 verankert. Für den Einsatz anderer Produkte wird eine Abklärung mit der ISS vorausgesetzt (siehe "8. Ausnahmen"). Die im Produktekatalog aufgeführten Komponenten werden gemäss den Richtlinien aus der IT-Architektur evaluiert, jährlich überprüft und wiederkehrend sowohl vom Regierungs- als auch vom Stadtrat bewilligt. Der Produktekatalog, die Standardkomponenten und der Dienstleistungskatalog dienen der Transparenz im IT-Umfeld, der Standardisierung und somit der Optimierung des Kosten-/Nutzenverhältnisses und der Sicherstellung der Nachhaltigkeit von Investitionen.

[2] Bei der Ausrüstung von Standardarbeitsplätzen wird die Thin-Client- und Server Based Computing-Strategie mit oberster Priorität verfolgt. Abweichungen werden nur mit dem im Kapitel 8. Ausnahmen beschriebenen Verfahren bewilligt.

[3] Die KSD wird die von ihr erworbenen Informatikmittel im Bereich Büroautomation (Standardarbeitsplatz) in einem Turnus von fünf bis acht Jahren (je nach Konfiguration) erneuern. Um die Budgetierung und die Wiederbeschaffung zu erleichtern, werden die Komponenten vermietet. Von der Miete ausgenommen sind Anschaffungen von Kleinmaterial wie Einzellizenzen, Scannern, etc. Die Budgethoheit für Kleinmaterial unterliegt den Dienststellen/Amtsstellen.

[4] Durch die zwingende Abwicklung der Beschaffung über die KSD wird dieser die Führung und Pflege eines verwaltungsweiten IT-Inventars und einer IT-Anlagebuchhaltung ermöglicht, was zusammen mit der Führung und Pflege eines Dienstleistungs- und Produktekataloges zu ihren Pflichten gehört. IT-Projekte, welche einen bestimmten Betrag übersteigen, sind per Antrag in das Projektportfolio aufzunehmen und unterliegen einem Bewilligungsverfahren.

[5] Aktuelle Informationen zum IT-Leitbild, zu den Budgetweisungen, zum Produktekatalog und den IT-Standards sind auf der Einsstiegsseite des Intranet-Portals zu finden.

4.2 Betrieb

[1] Im SHNet wird lediglich der Einsatz von Geräten, Plattformen und Software zugelassen, welche im Produktekatalog oder den IT-Standards aufgeführt sind oder schriftlich durch die KSD oder die ISS bewilligt wurden. Jegliche Software muss nachweisbar und ordnungsgemäss lizenziert sein. Die Anbindung von Geräten an das SHNet erfolgt ausschliesslich über die KSD. Damit wird sichergestellt, dass einerseits keine ungenügend geschützten Komponenten (Viren, Spionagesoftware, Servicepacks, etc.) betrieben werden und andererseits die Inventarisierung auf einem aktuellen Stand gehalten werden kann. Änderungen an Konfigurationen oder der Ein- bzw. Ausbau von IT-Komponenten sind nur in Absprache mit der KSD zulässig.

[2] Störungen des IT-Betriebs können innerhalb der ordentlichen Betriebszeiten (siehe Intranet-Portal) dem zentralen Helpdesk entweder telefonisch oder per E-Mail mitgeteilt werden (siehe "2. Verhalten bei IT-Störungen und IT-Notfällen").

[3] Garantiefälle bei Standardkomponenten, welche durch die KSD beschafft oder betrieben werden, müssen zwingend über die KSD abgehandelt werden.

4.3 Ersatz / Entsorgung / Verkauf

[1] Der Ersatz von IT-Geräten erfolgt periodisch nach 5 bis 8 Jahren gemäss Budgetierung und je nach Komponentenart. Die Dienststellen/Amtsstellen werden vorgängig kontaktiert und informiert. IT-Geräte mit Speichermedien oder Speichermedien selbst müssen vor deren Weitergabe an Dritte bzw. deren Veräusserung oder Entsorgung durch die KSD soweit behandelt werden, dass eine Wiederherstellung der Daten durch Unbefugte nicht mehr möglich ist. Detaillierte Informationen zur Veräusserung von IT-Geräten sind bei der KSD erhältlich und werden über das Dokument "Richtlinie zum Verkauf von gebrauchten IT-Geräten" abgehandelt (siehe Intranet-Portal).

[2] Die Entsorgung, Veräusserung oder örtliche Verschiebung von IT-Geräten, welche mit einer Inventarnummer der KSD versehen sind, muss vorgängig der KSD mitgeteilt werden, da nur so die Aktualität der Inventardaten gewährleistet ist.

[3] Softwarelizenzen sind nicht an Geräte gebunden und bleiben demzufolge auch nach der Veräusserung Eigentum des Arbeitgebers.

4.4 Private Hard- und Software

Aus Sicherheits- und Urheberrechtsgründen ist es den Mitarbeitenden untersagt, ohne Einbezug der KSD Software aus dem Internet herunter zu laden oder anderweitig fremde/private Produkte (Software und/oder Hardware wie beispielsweise private Wechseldatenträger) auf seinem Computer zu installieren und zu verwenden. Zudem dürfen Betriebs- und Applikationsprogramme ohne entsprechende Lizenz nicht anderweitig installiert werden (siehe "IT-Sicherheitsreglement", Kapitel privater Einsatz von Informatikmitteln sowie Weisung "Sicherer Arbeitsplatz").

5. Umgang mit elektronischen Informationen

5.1 Datenklassifizierung

[1] Um Daten respektive Informationen angemessen schützen und sichern zu können, müssen sie klassifiziert sein. Nicht alle Informationen sind gleich zu behandeln. Daten mit hoher Einstufung (vertrauliche Daten wie Geschäftsgeheimnisse oder Personendaten) werden höhere Prioritäten zugewiesen.

[2] Die Klassifizierungen gehören zu den Aufgaben des Dienststellenleiters/Amtsstellenleiters. Die KSD kann hierbei Unterstützung leisten, kann jedoch mangels ungenügender Einsicht und Know-how des entsprechenden Dienstbereiches diese nicht in Eigenregie durchführen.

[3] Zum Zweck der Datenklassifizierung wurde von der KSD eine Weisung "zur Klassifizierung von elektronischen Datenbeständen" erarbeitet, welche mit dem Regierungsratsbeschluss Nr. D/Sp/19/12 vom 9. Mai 2006 sowie dem Stadtratsbeschluss Nr. 218 vom 23. Mai 2006 verabschiedet wurde (siehe Intranet-Portal).

5.2 Datenschutz

[1] Unter Datenschutz wird der Schutz personenbezogener Daten vor missbräuchlicher Verwendung verstanden (Schutz der Privatsphäre).

[2] Die Aufgabe der KSD in diesem Zusammenhang besteht darin, sowohl organisatorische als auch technische Massnahmen soweit zu erarbeiten und bereitzustellen, dass der Schutz der Daten auf den zentralen Netzlaufwerken (Abteilungs- und Mitarbeiterdaten) den Anforderungen der Dienststellen/Amtsstellen entsprechend gewährleistet ist.

[3] Es ist jedoch Aufgabe der Dienststellenleiter/Amtsstellenleiter, den Umgang seiner Mitarbeitenden mit vertraulichen Daten zu definieren und zu kontrollieren (z.B. wie werden vertrauliche Daten versendet, abgelegt oder vernichtet).

5.2.1 Authentifikation an Systemen und Applikationen

5.2.1.1 Passwort

[1] Das Passwort oder auch Kennwort genannt, dient der Authentifizierung des Mitarbeitenden. Zusammen mit dem Benutzernamen regelt es die Zugriffsrechte auf Ressourcen innerhalb eines Netzwerkes sowie in Applikationen. Ein Passwort muss zum persönlichen Schutz streng vertraulich behandelt werden und darf weder an Stellvertreter oder Dritte übertragen, noch unmittelbar in der Nähe des Arbeitsplatzes notiert werden. Passwörter, welche durch die KSD für einen Supportfall angefordert werden, dürfen nur nach Rückruf an den Helpdesk ausgehändigt werden und sind nach Beendigung der Hilfestellung umgehend zu ändern. Das Passwort muss eine genügende Komplexität aufweisen und regelmässig geändert werden. Der Passwortschutz wird nach Ablauf einer bestimmten, beschränkten Dauer durch den Bildschirmschoner aktiviert, um eine Reauthentifizierung zu erwirken. In Anbetracht der Vielzahl von Passwörtern, welche von einem einzelnen Benutzer in Erinnerung behalten werden müssen, ist die Benutzung einer verschlüsselten Passwortdatenbank statt einer Passwortliste in Papierform zu empfehlen. Die KSD empfiehlt auf Wunsch eine entsprechende Softwarelösung.
Detaillierte Informationen zum Umgang und der Definition von Passwörtern finden Sie in der Richtlinie "Sicheres Passwort" (siehe Intranet-Portal).

[2] Die Dienststellenleiter/Amtsstellenleiter sind verantwortlich, dass die Meldung von Ein- bzw. Austritten von Mitarbeitenden schriftlich mittels des im Intranet-Portal veröffentlichten Formulars erfolgt. Bei Neueintritten muss das Formular spätestens zehn Arbeitstage vor Arbeitsbeginn des neuen Mitarbeitenden bei der KSD vorliegen um rechtzeitig Benutzername, Passwort und die damit verbundenen Berechtigungen bereitstellen zu können.

5.2.2 Datenzugriff / Berechtigungen

[1] Der Zugriff auf Anwendungen und Daten wird grundsätzlich über die Mitgliedschaft in Berechtigungsgruppen und/oder –Rollen geregelt. Die Mitarbeitenden werden in die zur Ausübung ihrer Tätigkeiten erforderlichen Berechtigungsgruppen und -Rollen aufgenom-

men. Für die logische Zuordnung der Mitarbeitenden zu den Berechtigungsgruppen und –Rollen ist die Dienststelle/Amtsstelle verantwortlich. Die Umsetzung auf den einzelnen Anwendungen und Systemen (Aufnahme der Anwender in die einzelnen Berechtigungsgruppen und –Rollen) erfolgt allein durch die KSD.
[2] Grundsätzlich werden keine Administratorenrechte erteilt. Befristete Ausnahmefälle sind per schriftlichem Antrag möglich und werden protokolliert (siehe "8. Ausnahmen").
[3] Zu Dokumentationszwecken wird eine Matrix der Zugriffsberechtigungen geführt, welche für die eigene Dienststelle/Amtststelle bei der KSD angefordert werden kann.
Die Administratoren der KSD (unterliegen der Schweigepflicht) besitzen auf allen Anwendungen, Daten und Systemen Audit-Rechte. Gründe für Audit-Rechte sind:

- Nachvollziehbarkeit von Systemzugriffen bei speziellen Ereignissen (Datenmanipulation, unerlaubte Systemzugriffe, etc.)
- Trendanalysen zu Planungszwecken
- Datensicherung und Wiederherstellung

5.3 Datensicherheit

[1] Datensicherheit hat zum Ziel, die Verarbeitung, die Speicherung und den Transport von Informationen so zu gestalten, dass deren Verfügbarkeit, Vertraulichkeit und Integrität in ausreichendem Mass sichergestellt wird. Datensicherheit bezeichnet somit das gemeinsame Ziel, Datenbestände und Systeme vor Gefahren und Bedrohungen zu schützen, Schäden zu vermeiden und Risiken zu minimieren.
[2] Die Aufgabe der KSD in diesem Zusammenhang besteht darin, sowohl organisatorische als auch technische Massnahmen soweit zu erarbeiten und bereitzustellen, dass die Datensicherheit den Anforderungen der Dienststellen/Amtsstellen entsprechend gewährleistet ist.
[3] Es ist jedoch Aufgabe der Dienststellen/Amtsstellen, die Anforderungen bezüglich Verfügbarkeit Vertraulichkeit und Integrität zu definieren und zu deklarieren. Dies geschieht in Zusammenarbeit mit der KSD.
[4] Die technischen Massnahmen bezüglich Verfügbarkeit im SHNet konzentrieren sich im Wesentlichen auf den Transport der Daten und deren gleichzeitigen Speicherung an zwei unterschiedlichen Standorten, wodurch ein Datenverlust nahezu ausgeschlossen werden kann.

5.3.1 Datenablage

Die Daten werden grundsätzlich nach den Kriterien
- abteilungsspezifische Geschäftsdaten
- persönliche Geschäftsdaten
- abteilungsübergreifende Geschäftsdaten

in verschiedene Verzeichnisstrukturen abgelegt. Dabei gelten folgende, für alle Mitarbeitenden verbindlichen Vorgaben, die im Detail im Standard "Datenablage" definiert sind (siehe Intranet-Portal):

Laufwerk für abteilungsspezifische Geschäftsdaten
Entspricht der Ablage aller abteilungsrelevanten Daten. Die Grundstruktur dieser Datenablage ist für alle Abteilungen identisch und gegeben. Abweichungen zu diesem Standard sind nicht möglich. Eine untergeordnete Ordnerstruktur kann durch die Abteilung in Eigenregie oder in Zusammenarbeit mit der KSD festgelegt werden. Die Struktur sieht verschiedene Ordner mit beschränkten Rechten vor, wie z.B. einen Ordner für die Geschäftsleitung, das Personalwesen, etc. Die Verantwortung der korrekten Datenablage liegt bei dem Vorgesetzten der Abteilung.

Laufwerk für persönliche Geschäftsdaten
Entspricht der Ablage für persönliche Geschäftsdaten der einzelnen Mitarbeitenden. Dazu gehören beispielsweise Spesenabrechnungen, Zeitkontrollblätter, etc. Änderungsberechtigung auf diesen Datenbereich hat nur der "Besitzer" der Daten.

Laufwerk für abteilungsübergreifende Geschäftsdaten
Entspricht der Ablage für Daten, welche ausserhalb der eigenen Abteilung zugänglich gemacht werden müssen. Ebenso können gemeinsame Ablagestrukturen für Kommissionen und Projektgruppen geschaffen werden.

5.3.2 Datensicherung

[1] Die KSD ist verantwortlich für die Sicherung aller Daten der von ihr betriebenen Datenbanken, Anwendungen und Systemen. Ebenso für die Sicherung aller Daten auf Netzwerklaufwerken im SHNet.
[2] Die KSD übernimmt keine Verantwortung für die Vertraulichkeit, Integrität und Verfügbarkeit von Daten, welche auf lokalen Datenträgern oder Wechseldatenträgern bei den Mitarbeitenden abgelegt sind.
[3] Die Datensicherung erfolgt nach zeitgemässen Techniken mit den entsprechenden Verfahren. Das Verfahren ist mehrstufig und gliedert sich wie folgt:

1. Sicherung auf Disk (Online-, Tages-, Wochen-, Monats- und Jahressicherungen) und Snapshots / Replikation
2. Kopie auf Band (Tages-, Wochen-, Monats- und Jahressicherungen)
3. Auslagerung von Bändern (Monats- und Jahressicherungen) in ein Bankschliessfach.

[4] Zur Sicherstellung der Wiederherstellung im Katastrophenfall werden regelmässig zusätzliche Sicherungen der Systemdateien und –dienste der verschiedenen Server und Systeme erstellt.

[5] Die Wiederherstellung von Daten ist grundsätzlich nicht kostenpflichtig. Eine Ausnahme bilden Rücksicherungen, welche ab Monatssicherungen (Daten älter als 4 Wochen auf Bändern im Bankschliessfach) wiederhergestellt werden müssen. Dieser zusätzliche Aufwand wird dem Auftraggeber in Rechnung gestellt (Minimalaufwand von einer Stunde).

6. Risiken, Bedrohungen und Schwachstellen

6.1 Bedrohungen

6.1.1 Malware

Als Malware bezeichnet man Computerprogramme, welche vom Mitarbeitenden unerwünschte (schädliche) Funktionen ausführen. Die Software läuft unbemerkt im Hintergrund. Schadfunktionen können zum Beispiel die Manipulation oder das Löschen von Dateien im System zur Folge haben. Zu Malware zählen Computerviren, Würmer, Trojanische Pferde und Spyware.

6.1.2 Social Engineering

Der Begriff Social Engineering bezeichnet zwischenmenschliche Beeinflussungen mit dem Ziel, unberechtigt an Informationen oder Gegenstände zu gelangen. Social Engineers spionieren das persönliche Umfeld ihres Opfers aus, täuschen falsche Identitäten vor oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus, um Dinge wie geheime Informationen oder unbezahlte Dienstleistungen zu erlangen. Meist dient Social Engineering dem Eindringen in ein fremdes Computersystem, um vertrauliche Daten einzusehen; man spricht dann auch von Social Hacking.

6.1.3 Phishing

Phishing (engl. phishing = abfischen) ist eine kriminelle Handlung, die Techniken des Social Engineerings verwendet. Phisher geben sich als vertrauenswürdige Personen aus und versuchen, durch gefälschte elektronische Nachrichten an sensible Daten wie Benutzernamen und Passwörter zu gelangen. Phishing-Nachrichten werden meist per E-Mail oder Instant Messaging versandt und fordern den Empfänger auf, auf einer präparierten Webseite oder am Telefon geheime Zugangsdaten preiszugeben.

6.1.4 Fehlende Vertraulichkeit

Trotz Einsatz verschiedener Firewall-, Antiviren- und Antispam-Systeme gelangen immer wieder unerwünschte Informationen in die Verwaltung. In den meisten Fällen kommen diese Nachrichten über das Medium E-Mail. Das Bedrohungsausmass variiert stark und kann deswegen nicht genau beziffert werden. Es kann sich um eine simple Werbung handeln, möglich wäre aber auch eine Attacke auf Unternehmensinformationen oder persönliche Angaben. Auch im Internet spielt die Vertraulichkeit eine grosse Rolle. Prinzipiell darf keinem Seiteninhalt vertraut oder keiner Aufforderung zur Bekanntgabe von persönlichen Daten Folge geleistet werden.

6.1.5 Anonymität

Bei Aktivitäten im Internet fühlen sich viele Benutzer anonym. Diese Anonymität ist jedoch trügerisch. Bei der Kommunikation erfährt die Gegenseite die eigene IP-Adresse, wodurch der Mitarbeitende identifiziert werden kann. Auch Cookies, Browserinformationen oder zuletzt besuchte Seiten können ohne Wissen des Mitarbeitenden weitergegeben werden. Die grösste Gefahr stellt der unbedarfte Umgang mit den eigenen Daten dar. Immer mehr Anwender geben Daten freigiebig für Bonussysteme wie Kundenkarten oder für Preisausschreiben bekannt, ohne zu wissen, was mit diesen geschieht.

Im Verwaltungsumfeld werden jegliche interne Informationen nach aussen so weit wie möglich geblockt. Eine vollumfängliche Anonymität wird jedoch mit allen im Einsatz stehenden Komponenten nicht erreicht.

6.2 Massnahmen

6.2.1 Verhalten des Benutzers

6.2.1.1 Verhalten am Arbeitsplatz

[1] Aus den vorhandenen Bedrohungen geht hervor, dass E-Mails welche von unbekannten, zusammenhangslosen Adressen eingehen und suspekten Inhalt aufweisen, eine grosse Gefahr für den Mitarbeitenden und die Verwaltung darstellen. Nur E-Mails oder Webinhalte von vertrauenswürdigen Anbietern dürfen akzeptiert werden. Persönliche Daten (auch die eigene Mailadresse) sollen nach Möglichkeit nicht preisgegeben werden. Kann nicht darauf verzichtet werden, muss auf eine verschlüsselte Client-Server-Verbindung geachtet werden (Mehr Informationen und Erklärungen siehe "7.3. Internet" unter "Sichere Verbindungen").

[2] Bedrohungen existieren nicht nur auf elektronischem Weg. Um einen sicheren Betrieb gewährleisten zu können, müssen die nachfolgenden Verhaltensregeln am Arbeitsplatz ebenfalls befolgt werden:

- Der Monitor am Arbeitsplatz soll so ausgerichtet sein, dass keine Einsicht von Dritten möglich ist.
- Zugangsdaten wie Benutzername und Passwort dürfen nicht aufgeschrieben, hinterlegt oder weitergeben werden.
- Beim Verlassen des Arbeitsplatzes ist die aktive Sitzung zu sperren oder die Abmeldeprozedur durchzuführen.

(Weitere wichtige Verhaltensregeln sind in der Weisung "Sicherer Arbeitsplatz" im Intranet-Portal publiziert.)

6.2.1.2 Verhalten ausserhalb der eigenen Büroräumlichkeiten (Arbeitsplatz)

[1] Die Möglichkeiten zur Erfüllung der täglichen Arbeit gestaltet sich immer flexibler. Mittels mobilen Endgeräten wie Notebook oder Smartphone ist die Erledigung der Arbeit auch ausserhalb der Büroräumlichkeiten gewährleistet. Diese Tatsache erfordert hohe Sicherheitsmechanismen und stellt immer wieder neue Anforderungen an Infrastruktur und Verhalten der Mitarbeitenden. Neben der Gewährleistung der Sicherheit auf technischer Seite, geht das bewusste Umgehen mit den Technologien durch die Mitarbeitenden oft vergessen.

[2] Ein sensibilisierter Umgang mit mobilen Endgeräten wird von allen Mitarbeitenden erwartet. Da auf den mobilen Endgeräten häufig

Kopien der E-Mails und Geschäftsdaten verfügbar sind, müssen diese mit besonderer Vorsicht verwendet und geschützt werden.
(Für weitere Hinweise siehe Weisung "Remote Arbeitsplatz" und Weisung "Mobile Endgeräte".)

6.2.2 Risikominimierung durch Informatikmittel

Die KSD betreibt diverse technische Hilfsmittel zur Minimierung von bestehenden Risiken und Bedrohungen. Dazu zählen:

6.2.2.1 Antivirenprogramme

Zum Schutz vor Viren, wird im SHNet ein mehrstufiges Antivirenkonzept mit unterschiedlichen Lösungen eingesetzt, welche die Einschleusung und Verbreitung von Viren verhindern soll. Die verwendeten Schutzmechanismen werden automatisch und permanent mit den neusten Virendefinitionen aktualisiert. Die Daten werden laufend auf unerlaubte Veränderungen überprüft. Es wäre jedoch trügerisch, sich nur auf diese Technologien zu verlassen. Beim Austausch von Daten über das Internet und beim Einsatz von fremden Datenträgern ist besonders darauf zu achten, dass der Urheber als vertrauenswürdige Person eingestuft werden kann. Bei Virenmeldungen, Unstimmigkeiten oder im Zweifelsfalle muss zwingend der Helpdesk der KSD informiert werden. Notebooks, PDA's und Smartphones, welche nicht regelmässig über das SHNet aktualisiert werden können, unterliegen einem erhöhten Risiko. Trotzdem sollte die letzte Aktualisierung der Virendefinitionen nicht länger als drei Tage zurück liegen.

6.2.2.2 Spamschutz

Die KSD überprüft anhand aktuellster Technologien eingehende E-Mails auf Spam.

6.2.2.3 Patchmanagement

Die mehrheitlich auf Windows und Linux basierenden Betriebssysteme unterliegen einer stetigen Aktualisierung durch so genannte Patches. Durch Patches werden in der Regel Sicherheitslecks und/oder Softwarefehler in Betriebssystemen und Softwarelösungen eliminiert. Die Verteilung dieser Softwareaktualisierungen wird nach einer Verifizierung durch die KSD im SHNet automatisch durchgeführt, ohne dass der Mitarbeitende in seiner Arbeit davon beeinträchtigt wird.

6.2.2.4 Personal Firewall
Eine Firewall dient der Vorbeugung und Verhinderung von unerlaubten Zugriffen durch unautorisierte Dritte auf fremde Daten und verhindert das Einschleusen oder die Verbreitung von Spionagesoftware. Solche Zugriffsversuche können durchaus auch aus dem eigenen Netz stattfinden. Um diese Risiken zu minimieren werden Personal Firewalls auf jedem einzelnen Client installiert und zentral verwaltet. Da sie aus Sicherheitsgründen bestimmte Transportkanäle im Netzwerk für die Kommunikation sperren, kann es als Einschränkung empfunden werden. Werden dadurch geschäftsrelevante Prozesse verhindert, kann bei der KSD ein Antrag auf deren Freischaltung gestellt werden (siehe Anhang).

7. Umgang mit Verbindungen

7.1 Interne Verbindungen

7.1.1 Physikalische Verbindungen
[1] Im Verwaltungsumfeld sind aus Sicherheitsgründen nur kabelgebundene Verbindungen mit dem SHNet und von Komponenten untereinander erlaubt. Verbindungen wie Wireless LAN, Wireless Ad-Hoc, Bluetooth, Infrarot und andere Funkverbindungen sind somit zu unterbinden (Die Aufzählung ist nicht abschliessend. Alle nicht erwähnten Verbindungsarten/-typen sind ebenfalls untersagt).
[2] Ausnahmen sind Funktastaturen, deren Kommunikation verschlüsselt übertragen wird und Funkmäuse. Die Beschaffung (siehe "4.1 Beschaffung") muss über die KSD erfolgen.
[3] Wireless Lan als Verbindungsmöglichkeit mit dem SHNet wird nur in Ausnahmesituationen bewilligt. Die Installation und Konfiguration muss zwingend durch die KSD erfolgen. Anderseits müssen Wireless-Schnittstellen bei einer kabelgebundenen Verbindung deaktiviert werden.

7.1.2 Logische Verbindungen
Der Zugriff vom Client auf eine Netzwerkfreigabe wird als logische Verbindung bezeichnet. Die Verbindung wird während des Anmeldeprozesses mittels Loginscript automatisch hergestellt und verbindet einen fix definierten Laufwerkbuchstaben mit der im Berechtigungs- und Zugriffskonzept definierten Netzwerkfreigabe und somit mit der darunter liegenden Datenstruktur. Die Erstellung eigener Freigaben ist strikte verboten, da diese weder dem Zugriffskon-

zept entsprechen, noch gesichert werden. Eine unautorisierte Netzwerkfreigabe kann dazu führen, dass Dritte vertrauliche Daten einsehen können. Ebenfalls untersagt ist das Durchsuchen (Scannen) fremder Netzwerkfreigaben.

7.2 Externe Verbindungen

[1] Die KSD betreibt diverse Systeme, die soweit möglich, eine sichere Kommunikation mit verwaltungsexternen Knoten gewährleisten. Systeme wie Firewalls blockieren Angriffe vom externen Netz und erlauben nur die definierten Zugriffe. Die im Einsatz stehenden Proxy-Server erhöhen Komfort und Sicherheit im Zusammenhang mit dem Internetzugang. Im Bereich der E-Mail-Kommunikation existieren zusätzliche Systeme, die vor Viren, Spam und anderen potentiellen Gefahren schützen.

[2] Datenverbindungen über Modems, GPRS oder andere Technologien öffnen unkontrollierbare Hintertüren in das SHNet und bedeuten eine grosse Bedrohung für die Verwaltung (z.B. Multifunktionsdrucker mit Faxunterstützung). Aus diesem Grund muss ge
mäss NSP-SH sowie RRB und SRB aus dem Jahre 1997 (Internet, Anschluss und Herstellung von Informationsseiten), "Jeder Verkehr mit offenen Netzen" über die KSD erfolgen. Jede nicht durch die KSD konfigurierte Verbindung ist demnach untersagt!
Ausnahmen sind GPRS-Verbindungen, die explizit von der KSD eingerichtet sind, wie zum Beispiel die Outlook-Synchronisation mit dem Smartphone (siehe auch Weisung "Mobile Endgeräte").
(Für weitere Informationen und Vorgaben siehe Vorgabe NSP-SH im Intranet-Portal)

7.3 Internet

Das Kommunikationsmittel Internet wird vom Arbeitgeber zur Erfüllung von geschäftlichen Aufgaben zur Verfügung gestellt. Es soll auch entsprechend genutzt werden.

Vertraulichkeit

Um sich so gut wie möglich zu schützen, sollten keine persönlichen Angaben – auch nicht die Mailadresse – im Internet preisgegeben werden. Für Newsletters, Wettbewerbe, Kauf- und Verkaufsangebote, Auktionen und Abonnemente, die keinen geschäftlichen Hintergrund aufweisen, darf die E-Mailadresse nicht verwendet werden.

Sichere Verbindungen (Zertifikate)

[1] Sichere Verbindungen werden im Browser mit dem Symbol  gekennzeichnet. Somit besteht eine sichere (verschlüsselte) Kommunikation zwischen Ihrem Computer und der Gegenstelle (Server/Applikation). Diese sicheren Verbindungen werden typischerweise in der Bankwelt für den elektronischen Zahlungsverkehr, aber auch für die Übermittlung von sensiblen Informationen, wie beispielsweise Personendaten verwendet. Persönliche Informationen dürfen nur über sichere Verbindungen oder verschlüsselt übermittelt werden.

[2] Durch Anklicken des  -Symbols kann das Zertifikat der Seite betrachtet werden. Im Zweifelsfall kann dadurch den Zusammenhang zwischen dem Seiteninhalt und der Organisation, die dieses Zertifikat beantragt hat, festgestellt werden.

Streaming
Das wiedergeben von Audio und Video über das Internet ist grundsätzlich nicht gestattet. In begründeten Ausnahmefällen kann bei der KSD eine Benutzerkennung (Benutzernamen und Passwort) angefordert werden, welche die entsprechende Person zur Nutzung der Streaming-Funktion berechtigt (siehe "8. Ausnahmen").

File-Download
Der File-Transfer über das Protokoll FTP ist nicht freigegeben. Um diesen Dienst nutzen zu können, muss ein Antrag an die KSD gestellt werden (siehe "8. Ausnahmen").

AntiVirus und Log
[1] Jeglicher Datenverkehr ins Internet wird von mehreren Geräten aufgezeichnet und kontrolliert. Alle unerlaubten Zugriffe werden in einem Log zusammengefasst und erlauben im Ereignisfall Rückschlüsse bis zum einzelnen Mitarbeitenden.
[2] Aktive Virenschutzmechanismen schützen die Unternehmung und den Mitarbeitenden vor Angriffen und infizierten Dateien.

Spezielle Zugriffe
Prinzipiell sind für Zugriffe in das Internet nur die Protokolle http und https erlaubt. Bei speziellen Anwendungen, die über eigene Ports in das Internet kommunizieren müssen, wird ein Antrag an die KSD erforderlich (siehe "8. Ausnahmen").

Unerlaubte Zugriffe
[1] Das Internet gehört, neben dem E-Mail-Verkehr, zu den grössten Gefahren für das Unternehmen. Unerlaubte Zugriffe zählen zu den grössten Bedrohungen und müssen bereits von den Mitarbeitenden vermieden werden.

[2] Zu unerlaubten Zugriffen gehören alle kostenpflichtigen Seiten, jeglicher Messaging- und Chat-Verkehr, alles im Zusammenhang mit Auktionen, Verkauf und Einkauf von Gütern, ausschliesslich des internen Markplatzes (http://marktplatz.ksd.ch), jegliche Spielseiten (hauptsächlich Glücksspiele mit Geldeinsätzen), sowie Finanztransaktionen. In jedem Fall verboten ist der Abruf von Webseiten mit erotischem, rassistischem oder gewalttätigem Inhalt, sowie Seiten, welche gegen die geltenden Gesetze, z. B. Strafgesetz oder Urheberrechtsgesetz, verstossen.
[3] Jegliches Ausführen von Scripts aus dem Internet ist verboten. Scripts führen unkontrollierbare Aktionen auf dem System aus, in vielen Fällen im Zusammenhang mit Viren.

7.4 E-Mail

Das Kommunikationsmittel E-Mail wird vom Arbeitgeber zur Erfüllung von geschäftlichen Aufgaben zur Verfügung gestellt. Es soll auch entsprechend genutzt werden.

Leeren des elektronischen Briefkastens (Abwesenheit)
Die Mitarbeitenden haben den elektronischen Briefkasten in der Regel täglich abzurufen. Im Falle einer Abwesenheit müssen Absender bzw. Empfänger einer E-Mail über die Abwesenheit und die Stellvertretungsregelung informiert werden. Mit Einwilligung des Mitarbeitenden kann auch die automatische Weiterleitung der elektronischen Post an die Stellvertretung aktiviert werden.

Kommunikationsmittel
Grundsätzlich sind für Antworten und Rückfragen dieselben Kommunikationsmittel wie für die entsprechenden Anfragen zu benutzen. Für vertrauliche Daten sind jedoch immer sichere Kommunikationskanäle zu verwenden (Übertragung nur mit Verschlüsselung oder nur im SHNet).

Verfassen von E-Mails
Für die geschäftliche Mailkorrespondenz gelten dieselben formalen Vorschriften wie für die übrige Geschäftskorrespondenz. Die Mitarbeitenden müssen gegenüber dem Empfänger immer Namen, betriebliche Funktion sowie betriebliche Adresse inklusive Telefonnummer und Mailadresse angeben. Der Versand von anonymen E-Mails ist verboten.

Innerbetriebliche Kommunikation

Es ist zu berücksichtigen, dass E-Mails nicht gegen den Betriebsfrieden verstossen, also weder Belästigungen noch Beleidigungen enthalten dürfen.

Massenversand
Ein Massenversand darf nur nach Rücksprache mit der KSD stattfinden und muss geschäftlichen Charakter besitzen. Das versenden von Werbung ist nicht gestattet.

Postfachgrösse
[1] Die Postfachgrösse ist limitiert. Wird die Grösse überschritten, wird der Benutzer automatisch vom System mit einem Mail darauf hingewiesen. Wird das Postfach danach nicht bereinigt, können keine Mails mehr vom Postfach versendet und zuletzt auch nicht mehr empfangen werden. Diese Begrenzung ist nötig, um in einem Desasterfall in einer zweckmässigen Zeit das System wiederherstellen zu können.
[2] Auch die maximale Grösse der zu versendenden Mails ist beschränkt.
[3] Das Mailsystem soll nicht als Aufbewahrungs- oder Archivsystem genutzt werden. Die E-Mails sind entsprechend ausserhalb des Postfaches abzulegen. Für die Konfiguration eines externen E-Mailordners ist die KSD gerne hilfsbereit.

Weiterleitung
Das Weiterleiten der Geschäftsmails an eine externe Mailadresse ist aus Sicherheitsgründen nicht erlaubt.

Abwesenheitsassistenten
Bei Abwesenheiten ist der Abwesenheitsassistent zu aktivieren, der mittels automatisch generierten Antwortmails auf ihre Abwesenheit hinweist. Der Aufbau und Inhalt des Abwesenheitsassistenten wird durch eine Dienstellenweisung definiert oder gemäss CDCI erstellt.

Verteilerliste
Die Verwaltung der Verteilerliste obliegt den Dienststellen/Amtsstellen (Nachführen, Aktualisieren). Auf Anfrage unterstützt die KSD gerne bei der Erstellung zentraler Verteilerlisten.

Endungen der Dateianhänge
Aus Sicherheitsgründen können diverse Endungen nicht vom Outlook geöffnet werden. Zu gefährdeten Endungen zählen: cmd, bat, com, exe, js, jse, msi, msp, reg, scf, sct, vb, vbe, vbs, wsc, wsf, wsh, pif, scr

Signatur
Der Aufbau der E-Mailsignatur wird von der Staats- oder Stadtkanzlei definiert und ist auf dem Intranet hinterlegt.

7.5 Private Nutzung

Die private Nutzungsmöglichkeit ist eine freiwillige, vom Arbeitgeber jederzeit widerrufbare Leistung. In erster Linie dienen die elektronischen Kommunikationsmittel der Erfüllung der geschäftlichen Aufgaben. Diese haben Priorität. Auf Zusehen hin wird jedoch im folgenden Umfang eine geringfügige private Nutzung toleriert.

Zeitrahmen
Eine zeitlich geringfügige private Nutzung wird toleriert. Sie soll jedoch wenn möglich ausserhalb der Arbeitszeiten, das heisst während den Pausen, über Mittag oder nach Feierabend stattfinden. Auf keinen Fall darf durch eine private Nutzung der elektronischen Kommunikationsmittel die Arbeitsleistung oder die Systemsicherheit beeinträchtigt werden.

Abrufen von Webseiten / Herunterladen von Dateien
Auch für die private Nutzung gelten dieselben Bestimmungen, wie unter Punkt 7.3 "Internet" festgehalten.

E-Mails
Privaten E-Mails ist eine Erklärung in Form einer privaten Signatur anzuhängen Diese muss die private Adresse und Telefonnummer enthalten, wodurch auf den privaten und persönlichen Charakter der E-Mail hingewiesen wird. Der Hinweis der vertraulichen Daten ist nicht erforderlich.

8. Ausnahmen

Anträge für Ausnahmen und Abweichungen vom Standard müssen mittels Formular über die KSD abgehandelt werden. Die KSD prüft in technischer und sicherheitsrelevanter Hinsicht die Anforderungen zu abweichenden Systemen und Lösungen und entscheidet in erster Instanz über die Bewilligung derselben. Wird die Ablehnung eines Antrages von der Dienststelle/Amtsstelle nicht akzeptiert, besteht die Möglichkeit in zweiter Instanz an die Informatik-Strategiestelle und dritter Instanz an den Stadt- und Regierungsrat zu gelangen. Ein Anspruch auf Abweichung besteht nicht.
(Formular zur Abweichung vom Standard siehe Anhang)

9. Inkrafttreten / Gültigkeit

Das vorliegende Reglement tritt per Regierungsratsbeschluss Nr. 45/871 vom 11. Dezember 2007 und Stadtratsbeschluss Nr. 614 vom 18. Dezember 2007 per sofort in Kraft. Es löst das alte Benutzungsreglement über die Büroautomation ab. Es wird allen betroffenen Mitarbeitenden zur Kenntnis gebracht und gilt per Regierungsrats- und Stadtratsbeschluss für alle Mitarbeitenden per sofort. Das Reglement behält Gültigkeit, bis vom Arbeitgeber Änderungen erlassen werden, welche wiederum allen Betroffenen zur Kenntnis zu bringen sind. Der Arbeitgeber kann auf Grund seines Weisungsrechtes jederzeit Anpassungen an geänderte Verhältnisse vornehmen. Es besteht grundsätzlich kein Rechtsanspruch auf den Internetzugang.

10. Abkürzungsverzeichnis

CD	Compact Disc (kompakte Scheibe)
DVD	Digital Versatile Disc (Digitale vielseitige Scheibe)
GIS	Geografisches Informationssystem
GPRS	General Packet Radio Service (Allgemeiner paket-orientierter Funkdienst)
ISS	Inormatik-Strategiestelle
KSD	Kanton und Stadt Schaffhausen Datenverarbeitung
PDA	Personal Digital Assistent (persönlicher digitaler Assistent [meistens elektronische Agenda])
RRB	Regierungsratsbeschluss
SRB	Stadtratsbeschluss
SHNet	Gemeinsames Verwaltungsnetz von Kanton, Stadt und Gemeinden Schaffhausen

Glossar

Abteilung	Organisationseinheiten von Kanton und Stadt Schaffhausen wie z.B. Dienststellen, Amtsstellen, Referate, Ämter, Kanzleien, Bereiche, etc. Diese Organisationseinheiten können eine oder mehrere Finanzstellen umfassen.
Active Directory (AD)	Verzeichnisdienst von Microsoft: Es ordnet verschiedenen Netzwerkobjekten wie Benutzern, Computern u.a. Eigenschaften zu und verwaltet diese

AdHoc	Ein drahtloses Netzwerk zwischen zwei oder mehr Endgeräten, die ohne feste Infrastruktur auskommen
Awareness	Bezeichnet das Bewusstsein gegenüber einem Sachverhalt
Black-/Whitelist	Schwarze/Weisse Liste: Liste von Personen oder Dingen, die gegenüber den nicht aufgeführten in irgendeiner Form benachteiligt/bevorzugt werden sollen
Bluetooth	Standard für die drahtlose Funkvernetzung von Geräten über kurze Distanz
Chat	plaudern, unterhalten: Bezeichnet elektronische Kommunikation zwischen Personen in Echtzeit
Cookie	bezeichnet Informationen, die ein Webserver zu einem Browser/Client sendet und dort abgespeichert werden, um später diese erneut zu verwenden
Client-Server-Verbindung	Verbindung zwischen einem Server und dem eigenen Computer (Client)
Datenbank	Elektronische Datenverwaltung
Disc	Festplatte/Massenspeichermedium
E-Learning	Elektronisch unterstütztes Lernen
Firewall	Eine Netzwerk-Sicherheitskomponente, die Netzwerkverkehr erlaubt oder verbietet
Gigabyte	Masseinheit, in der Datenmengen gemessen werden
Hacker	Jemand, der unerlaubt in fremde Computer- und Netzwerksysteme eindringt
IP-Adresse	Eindeutige Adresse eines Gerätes im Netzwerk
Infrarot	Drahtlose Kommunikation über Wellenlängenbereich; Kommunikation nur über sehr kurze Distanz, mit Sichtkontakt
Instant Messaging	Ist ein Dienst, der es ermöglicht, in Echtzeit mit anderen Teilnehmern zu kommunizieren (chatten)
Know-how	Wissen (hinsichtlich eines bestimmten Anwendungsbereichs)
Log	Automatisch erstelltes Protokoll aller oder bestimmter Aktionen von Prozessen auf einem Computersystem
Loginscript	Abfolge von Befehlen, die beim Anmelden am System ausgeführt werden (u.a. um die Netzlaufwerke zu verbinden)

Malware	(siehe Bedrohungen "6.1.1 Malware")
Modem	Dient dazu, digitale Daten in für eine analoge Leitung geeignete Signale umzuwandeln. Wurde vor allem früher zur Verbindung mit dem Internet verwendet
Netzlaufwerk	Freigegebenes Laufwerk (Ordner) auf einem zentralen Server, worauf mittels virtuellen Laufwerks vom lokalen Computer zugegriffen wird
Netzwerkfreigabe (Freigabe)	(siehe Netzlaufwerk)
Newsletter	Ein meist elektronisches Rundschreiben
Notebook	Kleiner tragbarer Computer (früher Laptop)
Patch	Flick: Eine Korrekturauslieferung für Software oder Daten, um z.B. Sicherheitslücken zu schliessen
Phishing	(siehe Bedrohungen "6.1.3 Phishing")
Proxy-Server	Ein Dienstprogramm, das im Datenverkehr vermittelt. Es macht den Datentransfer effizienter bzw. schneller, kann aber auch durch Einsatz von Zugriffskontrollmechanismen die Sicherheit erhöhen.
Quotas	Begrenzung des Speicherplatzes auf Speichermedien wie z.B. Festplatten pro Benutzer/Gruppe
Raid-System	Dient zur Organisation mehrerer Festplatten, um eine grössere Speicherkapazität, eine höhere Datensicherheit bei Ausfall einzelner Festplatten und/oder einen grösseren Datendurchsatz zu erreichen
Redundanz	Bezeichnet das mehrfache Vorhandensein von Objekten (wird aus Sicherheitsgründen erzeugt)
Replikation/ Replizierung	Bezeichnet die mehrfache Speicherung von Daten an typischerweise unterschiedlichen Standorten.
Server Based Computing	Bietet die zentrale Bereitstellung von Client/Server-Anwendungen auf leistungsfähigen Servern
Servicepack	Bezeichnet die Zusammenstellung von Patches zu einem Paket zur Aktualisierung des Betriebssystems oder installierten Produkten
Single point of contact	Bezeichnet eine exklusive Anlaufstelle für ein bestimmtes Thema oder Problem. (In der IT z.B. der Helpdesk als Schnittstelle für alle Problemfälle)

Smartphone	Mobiltelefon mit grösserem Leistungsumfang (Synchronisation von Terminen, E-Mails, Internet, etc.)
Snapshot	Eine Variante, nur die Änderungen von Dateien zum Original aufzuzeichnen (zusammen mit der Originaldatei kann die Datei wiederhergestellt werden).
Spam / Junk	unerwünschte, nicht verlangte und in der Regel auf elektronischem Weg übertragene E-Mails
Social Engineering	(siehe Bedrohungen "6.1.2 Social Engineering")
Streaming	Bezeichnet das Empfangen und gleichzeitige Wiedergeben von Audio- und Videodaten
Thin Client	Bezeichnet einen Computer als Endgerät (Terminal) eines Netzwerkes, dessen funktionale Ausstattung auf die Ein- und Ausgabe beschränkt ist
USV-Anlage	Mit Akkus betriebene Notstromanlage
Verschlüsselung	Bezeichnet den Vorgang, bei dem ein klar lesbarer Text (Klartext) mit Hilfe eines Verschlüsselungsverfahrens (Kryptosystem) in eine „unleserliche“, das heisst nicht einfach interpretierbare Zeichenfolge (Geheimtext) umgewandelt wird
(Wechsel) datenträger	(nicht fest eingebautes, sondern austauschbares, meist mobiles) Speichermedium
Wireless Lan	Drahtloses Funknetzwerk
Zertifikat	Sind strukturierte Daten, die den Eigentümer sowie weitere Eigenschaften eines öffentlichen Schlüssels bestätigen (siehe "7.3. Internet" unter "Sichere Verbindung (Zertifikat)")