PAUL SCHERRER INSTITUT	Registrierung AW-95-06-01 Rev. 1
Titel: Nutzung und Überwachung der EDV-Ressourcen am PSI	Ersetzt AW-95-06-01
Autoren / Autorinnen: Tobias Marx / Werner Roser / Karsten Bugmann	Erstellt 11.12.2013

Zusammenfassung:

Diese Weisung definiert die Nutzung und Überwachung sämtlicher EDV-Ressourcen am PSI für alle Benutzerinnen und Benutzer.

Die Revision 1 dieser Weisung wurde an der Direktionskonferenz vom 11.12.2013 genehmigt und per 1.2.2014 in Kraft gesetzt.

Verteiler	Abt.	Empfänger / Empfängerinnen	Expl.	Abt.	Empfänger / Empfängerinnen	Expl.
	PSI	Information aller PSI-MA über die Linie und Hinweis im PSI-Aktuell auf den Link im Intranet! Neueintretende erhalten den Link am 1. Arbeitstag.	1	Linienvorgesetzte aller Stufen und PSI-Kontakt-person	Verteilung an temp. Mitarbeiter und Mitarbeiter von Fremdfirmen, Aushilfen, Praktikanten und Gästen etc. Publikation im Intranet	
	User-Office	ExperimentatorInnen via „Digital User Office“				

	Expl.
Bibliothek	3
Reserve	
Total	
Seiten	4
Beilagen	

Informationsliste

D	1	2	3	4	5	8	9	A

Visum Abt.-/Laborleitung: ES95

Diese Weisung beschreibt die Regeln für den Umgang mit EDV-Ressourcen am PSI. Die Regeln sind bindend für alle Benutzerinnen und Benutzer, die jegliche Arten von EDV-Ressourcen (PCs, Netzwerke, Modems etc.) des PSI nutzen.

1. Nutzung der EDV-Ressourcen

Jede Benutzerin und jeder Benutzer ist persönlich dafür verantwortlich, dass die Benutzung der PSI EDV-Ressourcen die Bestimmungen dieser Weisung, die Rechtsordnung (z. B. Strafrecht, Datenschutz etc.) und die Rechte Dritter (Urheberrechte, Lizenzbestimmungen, Persönlichkeitsrechte) nicht verletzen. Die Benutzung von PSI EDV-Ressourcen darf dem Ruf des PSI nicht schaden.

Die EDV-Ressourcen des PSI dienen primär der Arbeit. Privater Gebrauch ist auf ein Minimum zu reduzieren. Private Daten sind dabei Dokumente aller Datentypen, inkl. E-Mails und Terminen, die keinen Bezug zum PSI oder zur Tätigkeit am PSI haben. Die private Nutzung von PSI EDV-Ressourcen darf nicht zu einer technischen Störung, Beeinträchtigung, oder zu einer unverhältnismässigen Beanspruchung von allgemein genutzten Ressourcen führen, und keinen kommerziellen Zweck verfolgen.

Private Daten müssen an den dafür vorgesehenen Speicherorten abgespeichert werden, damit die Privatsphäre geschützt werden kann. Private Daten müssen dazu in mit „privat“ bezeichneten (Unter-)Ordnern abgespeichert werden. Alle anderen Daten müssen ausserhalb dieser Speicherorte abgespeichert werden.

Darüber hinaus dürfen keine privaten Webinhalte mit Hilfe der PSI EDV-Ressourcen veröffentlicht werden. Ausgenommen hiervon sind Angaben zu persönlichen Werdegängen und Publikationen. Hierfür sind vorhandene PSI-spezifische Design-Vorgaben (Corporate Design) zwingend anzuwenden.

Im Falle längerer Abwesenheit oder Nichtverfügbarkeit von Zugriffsberechtigten und deren Stellvertreter kann den Vorgesetzten des betroffenen Mitarbeiters nach Genehmigung durch den Leiter Personalmanagement und den Sicherheitsdelegierten, resp. deren Stellvertreter, das Zugriffsrecht auf die **funktionsbezogenen** Daten gegeben werden, sofern dieser Zugriff sich aus PSI-Sicht als notwendig erweist. Funktionsbezogene Daten sind hierbei Daten auf die im Regelfall nur eine Person resp. die von dieser Person bestimmten Stellvertreter Zugriff haben. Für den Zugriff auf **private** Daten ist zusätzlich die Erlaubnis eines der nächsten Angehörigen erforderlich.

2. Missbrauch

Missbräuchlich ist jede Nutzung der PSI EDV-Ressourcen, die die Vorgaben dieser Weisung missachtet, gegen übergeordnetes Recht verstösst oder die Rechte Dritter verletzt.

Als missbräuchlich gelten insbesondere die folgenden Verhaltensweisen, die im Anhang dieser Weisung ggf. detaillierter erläutert sind:

a) Der Besuch von pornographischen, sexistischen, rassistischen und ehrverletzenden Webseiten, ebenso die Aufbewahrung und Verteilung derartiger Inhalte.
b) Die Belästigung von PSI Mitarbeitenden oder Drittpersonen durch Mitteilungen mit elektronischen Kommunikationsmitteln.
c) Das Versenden von Werbe-E-Mails (Spam) oder Phishing-E-Mails.
d) Die Verwendung von Programmen ohne gültige Lizenz auf PSI-Systemen, sowie Verstösse gegen das Urheberrecht.
e) Das absichtliche Umgehen von netzwerkseitigen Kontrollmechanismen des PSI.
f) Jegliche Arten der Nutzung der PSI-Netzwerke, die nicht von der AIT genehmigt wurde.
g) Jede Nutzung der PSI EDV-Ressourcen, die die IT-Sicherheit, die allgemeine Sicherheit oder weitere EDV-Ressourcen des PSI schädigt.

3. Schwerer Missbrauch

Als schwere Missbräuche gelten die folgenden Verhaltensweisen, die im Anhang dieser Weisung ggf. detaillierter erläutert sind:

a) Verstösse gegen Artikel des geltenden StGB, soweit diese vorsätzlich bzw. absichtlich erfolgen.
b) Missbräuche gemäss Absatz 2. im Wiederholungsfall.
c) Jede Nutzung der PSI EDV-Ressourcen, die den Ruf des PSI beschädigt.

Die Kenntnis schwerer oder wiederholter missbräuchlicher Nutzung verpflichtet die direkten Vorgesetzten, sowie die System- und Netzwerkverantwortlichen zur Meldung an die Leitung des Personalmanagements.

4. Überwachungsregelung und Konsequenzen

Der gesamte Netzwerkverkehr zwischen den PSI-Netzwerken und dem Internet wird zwecks Kontrolle der Einhaltung der Nutzungsrechte überwacht und aufgezeichnet. Aus Sicherheitsgründen und zur Qualitätssicherung werten autorisierte AIT-Mitarbeiter die Aufzeichnungen und Überwachungsprotokolle anonymisiert aus. Bei festgestelltem Missbrauch oder einem begründeten Verdacht auf missbräuchliche Nutzung der PSI EDV-Ressourcen erfolgt eine Meldung an die Leitung des Personalmanagements. Diese kann eine personenbezogene Auswertung anfordern. Im Falle von schwerem Missbrauch darf der Fachspezialist für IT-Sicherheit auch die möglicherweise am Missbrauch beteiligten Computersysteme einsehen.

Erhärtet sich der Verdacht auf missbräuchliche Nutzung nicht, wird die namentliche Auswertung aller Protokolle unverzüglich eingestellt und die Unterlagen werden vernichtet.

Die Feststellung eines Missbrauchs - oder der begründete Verdacht eines Missbrauchs - im Sinne dieser Weisung kann zu administrativen Massnahmen und zum temporären Verlust des Nutzungsrechtes der EDV-Ressourcen führen. Die an einem Missbrauch beteiligten Systeme können vom Netz genommen werden und erhalten erst wieder einen Zugang, wenn die Sicherheit wieder hergestellt und/oder der Missbrauch beendet wurde.

Wenn eine Straftat festgestellt oder vermutet wird, sichert das PSI die entsprechenden Protokollierungen. Das PSI behält sich das Recht vor, Anzeige gegen die betroffenen Personen zu erstatten. Für die weitere Beurteilung von Sachverhalten im Zusammenhang mit der Nutzung von PSI EDV-Ressourcen (insbesondere der missbräuchlichen Nutzung) gilt Schweizerisches Recht.

In allen Fällen von schwerem Missbrauch beurteilen die Linie, die Leitung des Personalmanagements und der Direktor gemeinsam personalrechtliche Massnahmen.

Die durch Missbräuche und deren Folgen, einschliesslich der Aufklärung und Sanktionierung, verursachten Kosten (inkl. Untersuchungs-, Gerichts- und Anwaltskosten), kann das PSI auf die fehlbaren Personen überwälzen.

Anhang

Erläuterungen zu Absatz 2. Missbrauch

Zu d)

Verstösse gegen das Urheberrecht sind die Benutzung, Beschaffung, Verteilung oder Speicherung urheberrechtlich geschützter Daten und Programme ohne entsprechende Bewilligung.

Zu e)

Hierunter ist die vorsätzliche Installation und Nutzung von Programmen/Techniken zu verstehen, die Netzwerkverbindungen aus dem Internet ins PSI-Netzwerk oder Netzwerkverbindungen aus dem PSI-Netzwerk ins Internet ermöglichen, und dabei die Kontrollmechanismen (z. B. Firewall) des PSI umgehen.

Zu f)

darunter verstehen wir u. a.:

- Die gleichzeitige Nutzung des PSI-Netzwerkes und des Gästenetzes auf demselben Gerät. Ebenso die gleichzeitige Nutzung des PSI-Netzwerkes und die Nutzung von öffentlichen WLANs/GPRS- und UMTS-Netzen etc. (bspw. Swisscom). Das heisst, sämtliche Netzwerkverbindungen zu Fremdnetzen sind während der Nutzung des PSI-Netzwerkes generell zu deaktivieren.
- Die Installation und das Betreiben von WLAN-Access-Points, die nicht von der AIT genehmigt wurden. Dies gilt auch für sämtliche WLAN-Komponenten im ad hoc Modus. Der so genannte ad hoc Modus ermöglicht eine direkte Verbindung mit anderen Computersystemen, und kann im Extremfall ein Zugang zum internen Netzwerk des PSI herstellen.
- Die Verbindung von privaten Computersystemen von PSI-Mitarbeitern und Gästen mit dem PSI-Netzwerk ohne ausreichende Virenschutzmechanismen und aller verfügbaren Sicherheitsupdates. Dies hat auch Gültigkeit für alle PSI-Systeme, die nicht von der AIT betreut, und für alle Systeme die mittels einer VPN-Verbindung mit dem PSI-Netzwerk verbunden werden (bspw. PC im privaten Haushalt, Notebooks etc.).
- Die Nutzung jeglicher Arten von Peer-to-Peer-Software (emule, edonkey, BitTorrent, etc.) zur Beschaffung von urheberrechtlich geschützten Daten (Filme, Musikdateien, Spiele, Software etc.), sowie gegen Art 197 StGB verstossendem Material.
- Die Weitergabe von persönlichen Passwörtern an Dritte für die Nutzung von PSI EDV-Ressourcen, sowie die ungesicherte Aufbewahrung von aufgeschriebenen Passwörtern, und die ungesicherte Speicherung von Passwörtern innerhalb von Dateien und Skripten, sofern die Passwörter einen Zugriff auf PSI EDV-Ressourcen ermöglichen.
- Das Veröffentlichen von PSI-internen Informationen im Internet ohne Passwortschutz.

Erläuterungen zu Absatz 3. Schwerer Missbrauch

Zu a)

Zu den Verstössen gegen Artikel des geltenden StGB zählen insbesondere:

- Verarbeitung, Erwerb, Speicherung, Übermittlung, das Anbieten, Zeigen, Überlassen und Zugänglichmachen von Material, wie z. B. Gewaltdarstellungen, sexuelle Handlungen im Sinne von Art. 197 Ziff. 3, 3^{bis} StGB. Die Aufforderung zu Verbrechen oder Gewalttätigkeit (Art. 259 StGB), Störung der Glaubens- und Kultusfreiheit (Art. 261 StGB) oder Rassendiskriminierung (Art. 261^{bis} StGB).
- Die Herstellung, Anleitung zur Herstellung oder absichtliche Verbreitung von schädlichen Programmen oder Programmteilen im Sinne von Art. 144^{bis} Ziff. 2 StGB (Viren, Würmer, Trojaner, etc).
- Das unbefugte Eindringen in ein Datenverarbeitungssystem (Art. 143^{bis} StGB) (Hacking), Ausspionieren von Passwörtern, Erschleichen von Passwörtern, Kreditkarten- oder Kontonummern (Phishing), unautorisiertes Absuchen von internen und externen Netzwerken auf Schwachstellen (z. B. Port-Scanning), Vorkehrungen und Durchführung von Massnahmen zur Störung von Netzwerken und Computern (Denial of Service).
- Datendiebstahl (Art. 143 StGB) und Datenbeschädigung (Art. 144^{bis} Ziff. 1 StGB).

Der Fachspezialist für IT-Sicherheit darf zur Überprüfung des Sicherheitsniveaus der PSI EDV-Ressourcen entsprechende Verfahren und Techniken anwenden.