UNIVERSITÄT BERN

Verwaltungsdirektion

Abteilung Informatikdienste

Richtlinien

Technik-Verantwortliche

Version	Bearbeitung	Ersteller	Datum
1.0	Neues Dokument	Christian Heim	28.07.2009
1.1	Überarbeitung	ID-Mini	01.04.2013
1.2	Überarbeitung	ID-Mini	18.02.2014
1.3	Review und Aktualisierung der Links	ID-Mini	01.03.2016
1.4	Review und Aktualisierung der Links	Beatrice Hirschi, Thushjandan Ponnudurai, Philipp Tobler	29.01.2019
1.5	Ergänzung Bereich Support	SMT	17.07.2019
1.6	Erweiterung Pflichten und Aufgaben	SMT	20.02.2020

Verteiler	Technik-Verantwortliche, Informatikdienste
Klassifikation	Für internen Gebrauch
Dokumentenstatus	Freigegeben

Informatikdienste
Hochschulstrasse 6
3012 Bern
Schweiz

Inhaltsverzeichnis

1. Grundsätzliches 3
1.1 Zweck der Richtlinie 3
2. Aufgaben 3
2.1 Bereich Netzwerk 3
2.2 Bereich Datensicherheit und Datenschutz 3
2.3 Bereich Support 4
3. Kompetenzen und Pflichten 4
4. Kontakte 5
5. Schlussbestimmungen 5
5.1 Widersprechende Bestimmungen 5
5.2 Inkrafttreten 5
6. Links 5

1. Grundsätzliches

1.1 Zweck der Richtlinie

Diese Richtlinien umschreiben die Aufgaben und Pflichten der Technik-Verantwortlichen der Organisationseinheiten. Im ersten Teil werden die konkreten Aufgaben in den einzelnen Tätigkeitsgebieten aufgeführt. Im zweiten Teil werden die Kompetenzen und Pflichten beschrieben.

2. Aufgaben

2.1 Bereich Netzwerk

- Beantragen der Aufschaltung von Netzwerkanschlüssen bei den Informatikdiensten [1]
- Legitimieren von Geräten für den Netzwerkanschluss
- Beantragen von IP-Adressbereichen
- Führen und kontrollieren der seiner Institution zugewiesenen IP-Adressen
- Anbindung von Netzwerkgeräten ans Uni-Netz gemäss "Weisungen über das Netzwerk der Universität Bern" [2]
- Lokalisieren und Beheben von Netzwerkproblemen
- Ansprechperson bei Netzwerkproblemen, sowohl innerhalb der Organisationseinheit wie auch gegenüber den Informatikdiensten
- Pflegen der Border Firewall-Regeln und DNS-Einträge im NetAdmin Portal [3]
- Bestellen von Netzwerkmaterial (Kabel und Mini-Switches) bei den Informatikdiensten [4]
- Anbindung von Clientsystemen (PCs/MACs und Drucker) an das Netzwerk
- Selbst administrierte Geräte gemäss Weisung "Weisungen zur Anbindung von privaten oder selbst administrierten IT-Geräten an das allgemeine universitäre Netzwerk" anbinden [2]

2.2 Bereich Datensicherheit und Datenschutz

- Regelmässiges Prüfen der Reports des ID-Schwachstellenscanners [3]
- Beheben der durch den ID-Schwachstellenscanner festgestellten Schwachstellen
- Aufsetzen und Konfigurieren einer sicheren IT-Infrastruktur (Virenschutz, Patches, Verschlüsselung)
- Beantragen und Verwalten von Service Accounts für automatisierte Aufgaben und Dienste auf Server-Systemen oder Applikationen gemäss Betriebskonzept Campus-Directory [5]
- Führen eines Inventars der vorhandenen IT-Infrastruktur mit den aktuellen Sicherheitseinstellungen (Betriebssystem-Release, Patch-Level, Virendefinition)
- Führen eines Inventars der vorhandenen Datenbestände mit den jeweiligen Schutzklassen gemäss Datenschutz
- Wo vorhanden, datenschutz-relevante Datenbestände mit entsprechender Sicherheit schützen
- Sicherstellen der korrekten Authentisierung und Autorisierung von lokalen Ressourcen
- Protokollierung der technischen Logdateien gemäss "Weisung über die Benutzung der IT-Ressourcen an der Universität Bern" [2]
- Sensibilisierung der Benutzenden auf Datenschutz, Schutz der IT-Infrastruktur vor Malware, Copyrights von Software und digitalen audiovisuellen Daten gemäss "Weisungen zum Datenschutz im IT-Bereich der Universität Bern" [2] sowie der Awareness-Schulung «IT-Sicherheit an der Universität Bern [6]

- Rapportieren von sicherheitsrelevanten Vorkommnissen in der IT-Infrastruktur des Institutes an die Institutsleitung und das Sicherheitsteam der ID (CSIRT)
- Verantwortlich für die Datensicherung relevanter Daten (Backup/Restore)

2.3 Bereich Support

- IT-Support (1st-Level) für Mitarbeitende der Organisationseinheit
- Einrichten und Konfigurieren der Geräte
- Neuinstallationen von PCs und MACs sowie Druckern
- Installation von Konfiguration von E-Mail-Clients
- Bestellen und Verwalten von SWITCHengines
- Regelmässige Kontrolle und Aktualisierung der Hard- und Software
- Installation von Sicherheitsupdates und Patches für die eingesetzten Softwareprodukte
- Sicherstellen, dass nur Systeme mit unterstützten, gewarteten Betriebssystemen am Uni-Netz betrieben werden
- Installation und Konfiguration von Antivirensoftware, inkl. Aktualisierung der AV-Signaturen
- Behebung von Hardware-Problemen und Störungen
- Leitet Informationen der Informatikdienste über Störungen oder Wartungsarbeiten nach eigenem Ermessen an die Mitarbeitenden weiter

3. Kompetenzen und Pflichten

- Die Technik-Verantwortlichen haben die Pflicht, bei Kenntnis schwerer oder wiederholter missbräuchlicher Verwendung der IT-Infrastruktur die Institutsleitung sowie das Sicherheitsteam der ID (CSIRT), Abs.4, zu informieren. Es wird empfohlen, vorgängig das Gespräch mit dem betreffenden Mitarbeitenden zu suchen und auf den Verstoss aufmerksam zu machen.
- Wird ein Missbrauch festgestellt oder besteht ein konkreter Verdacht, dürfen Massnahmen wie Sperrung von Konten oder personenbezogene Log-Auswertungen in Absprache mit dem Sicherheitsteam der ID (CSIRT) erfolgen.
- Die Mitarbeitenden sollen wiederholt darauf aufmerksam gemacht werden, dass die Nutzung der IT-Infrastruktur nur für den Zweck erlaubt ist, der in den "Weisungen über die Benutzung der IT-Ressourcen" [2] genannt ist. Missbräuchliche Nutzung wird sanktioniert.
- Der Stelleninhaber ist verantwortlich, dass bei Stellvertretung oder Stellenübergabe die institutsspezifischen Informationen nicht verloren gehen.
- Abtretende Stelleninhaber melden zusammen mit dem geschäftsführenden Organ der Organisationeinheit den neuen Technik-Verantwortlichen über das offizielle Formular "Kontaktadressen ändern" [7].
- Der/die Stelleninhaber/in ist zuständig für die physische Sicherheit von Serverräumen seiner Organisationseinheit. Darunter fallen auch die Zutritts-Sicherung und die Zutritts-Kontrolle.
- Anwendungen und Systeme mit erhöhtem Schutzbedarf müssen mit entsprechenden Mitteln geschützt werden. Bei Sicherheitsproblemen mit solchen Systemen muss eine Meldung an das Sicherheitsteam der ID (CSIRT) erfolgen.
- Technische Logdateien von Serverdiensten müssen für sechs Monate aufbewahrt werden und dem Sicherheitsteam der ID (CSIRT) zugänglich gemacht werden.
- Bei technischen Problemen kann der Technik-Verantwortliche Log files beiziehen und auswerten um die Ursache zu klären. Eine personenbezogene Auswertung ist strikte untersagt.
- Der Zugriff oder die Einsicht in Dokumente, die für die Arbeit des Technik-Verantwortlichen nicht relevant sind, ist strikte untersagt.

- Inhalte von E-Mails Dritter dürfen nicht überprüft oder zur Kenntnis genommen werden.
- Der Einsatz eines Passwort-Cracker Tools oder Key Logger auf Geräten von Mitarbeitenden ist ohne deren ausdrückliches Einverständnis nicht gestattet.
- Aufgezeichnete Randdaten sind als vertraulich zu beachten und müssen vor dem Zugriff durch Unberechtigte geschützt werden.
- Der Technik-Verantwortliche darf in seinem Verantwortungsbereich ein Scanning nach Verwundbarkeiten (port-scan oder weiterführende Techniken) durchführen mit dem Ziel, diese zu beseitigen.
- Elektronische Datenträger, die nicht weiterverwendet werden, sind entsprechend den "Richtlinien Sichere Entsorgung von IT-Datenträgern" zu entsorgen [2].
- Erfahrung im Bereich Active Directory, Windows File Services, Gruppenrichtlinien und Microsoft Office wird vorausgesetzt
- Verfügbarkeit / Erreichbarkeit für den Nutzenden soll gewährleistet sein
- Bei Abwesenheit soll eine Stellvertretung definiert werden
- Selbständige Informationsbeschaffung über Protokolle der ID-BEKO (Benutzerkonferenz)

4. Kontakte

Die Informatikdienste stehen den Technik-Verantwortlichen bei Fragen und Unklarheiten als 2nd Level Supportpartner zur Verfügung.

ID Helpdesk	Tel: 4999	E-Mail: helpdesk@id.unibe.ch
ID Sicherheitsteam (CSIRT)	Tel: 5455	E-Mail: csirt@unibe.ch
ID Netzwerk-Team	Tel: 5999	E-Mail: noc@unibe.ch

5. Schlussbestimmungen

5.1 Widersprechende Bestimmungen

Bestehende, diesen Richtlinien widersprechende Bestimmungen werden hiermit aufgehoben.

5.2 Inkrafttreten

Diese Richtlinien treten per sofort in Kraft.

6. Links

[1] http://id.intern.unibe.ch/formulare: Netzwerkanschluss bestellen
[2] http://id.unibe.ch/rechtssammlung
[3] https://netadmin.unibe.ch
[4] http://id.intern.unibe.ch/formulare: Netzwerkmaterial bestellen
[5] http://id.intern.unibe.ch/betriebskonzepte
[6] https://www.unibesecure.unibe.ch/
[7] http://id.intern.unibe.ch/formulare: Kontaktadressen ändern

Informatikdienste der Universität Bern

Bern, 20.02.2020

Leiter Informatikdienste