

Richtlinien für Technik-Verantwortliche

Die folgenden Richtlinien sollen mithelfen, die Aufgaben und Pflichten der IT-Verantwortlichen im technischen Bereich (Technik-Verantwortliche) der Organisationseinheiten zu umschreiben. Im ersten Teil werden die konkreten Aufgaben in den einzelnen Tätigkeitsgebieten des Technik-Verantwortlichen aufgeführt. Im zweiten Teil werden weitere generelle Pflichten und Verantwortlichkeiten behandelt.

1. Aufgaben

1.1 Bereich Netzwerk

- Beantragen von Anschlussgesuchen bei den ID
- Legitimieren von Geräten für den Netzwerkanschluss
- Ist verantwortlich für das zugeteilte Subnetz
- Beantragen von IP-Adressen beim Hostmaster der ID
- Führt und kontrolliert regelmässig die Liste der IP-Adressen (gemäss DNS-Richtlinie)
- Anbindung von Netzwerkgeräten ans UniNetz
- Beheben und lokalisieren von Netzwerkproblemen an Endgeräten
- Ansprechperson bei Netzwerkproblemen, sowohl innerhalb der Organisationseinheit wie auch gegenüber der ID
- Pflege der AUBEng-Einträge
- Regelmässiges Prüfen der Reports des ID-Sicherheitsscanners (Nessus)
- Bestellung von Netzwerkmaterial bei den ID

1.2. Bereich Datensicherheit und Datenschutz

- Beheben der durch den ID-Sicherheitsscanner festgestellten Schwachstellen
- Aufsetzen und Konfigurieren der IT-Infrastruktur unter Beachtung der sicherheitsrelevanten State of the Art Standards (Virenschutz, lokale Firewall, Patches, Verschlüsselung)
- Führen eines Inventars der vorhandenen IT-Infrastruktur mit den aktuellen Sicherheitseinstellungen (Betriebssystem-Release, Patch-Level, Virendefinitionen)
- Führen eines Inventars der vorhandenen Datenbestände mit den jeweiligen Schutzklassen gemäss Datenschutz
- Datenschutz-relevante Datenbestände mit entsprechenden Massnahmen schützen
- Pflege von Benutzerdatenbanken zur Authentisierung und Authorisierung von lokalen Ressourcen
- Protokollierung der Randdaten gemäss Weisungen der Universitätsleitung
- Sensibilisierung der Benutzer auf Datenschutz, Schutz der IT-Infrastruktur vor Malware, Copyrights von Software und digitalen audiovisuellen Daten gemäss Weisungen der Universitätsleitung
- Rapportieren von sicherheitsrelevanten Vorkommnissen in der IT-Infrastruktur des Instituts an Institutsleitung und das Sicherheitsteam der Informatikdienste
- Verantwortlich für die Datensicherung relevanter Daten (Backup/Restore)

1.3 Bereich Support

- IT-Support (1-st Level) für Mitarbeitende der Organisationseinheit
- Einrichten und Konfigurieren der Geräte nach entsprechenden Richtlinien
- Neuinstallationen von PCs und Macs sowie Druckern
- Installation und Konfiguration von EMail-Clients
- Regelmässige Kontrolle der Geräte sowie Installation von Sicherheitsupdates und Patches
- Installation und Konfiguration von Antivirensoftware
- Beheben von Hardware-Problemen und Störungen

2. Kompetenzen und Pflichten

1. Grundsätzlich besteht die Pflicht, bei Kenntnis schwerer oder wiederholter missbräuchlicher Verwendung der IT-Infrastruktur die Institutsleitung und zusätzlich das Sicherheitsteam der ID zu informieren. Es wird empfohlen, vorgängig das Gespräch mit dem betreffenden Mitarbeitenden zu suchen und diesen zu verwarnen.
2. Wird ein Missbrauch festgestellt oder besteht ein konkreter Verdacht, dürfen Massnahmen wie Sperrung von Konten oder personenbezogene Log-Auswertungen nur in Absprache mit dem Sicherheitsteam der ID erfolgen.
3. Die Mitarbeitenden sollen wiederholt darauf aufmerksam gemacht werden, dass die Nutzung der IT-Infrastruktur nur für diejenigen Zwecke erlaubt ist, die in den Weisungen über die Benutzung der Informatikmittel erwähnt sind und dass missbräuchliche Nutzung sanktioniert wird.
4. Der Stelleninhaber ist dafür verantwortlich, dass bei Stellvertretung oder Stellenübergabe die institutsspezifischen Informationen nicht verloren gehen.
5. Abtretende Stelleninhaber melden zusammen mit dem geschäftsführenden Organ der Organisationseinheit bei Stellenübergabe den neuen Technik-Verantwortlichen über das offizielle Meldeverfahren.
6. Der Stelleninhaber ist zuständig für die physische Sicherheit von Serverräumen seiner Organisationseinheit. Darunter fällt auch die Zutrittssicherung und die Zutrittskontrolle.
7. 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 erfolgen.
8. Randdaten (logfiles) von Serverdiensten müssen gemäss Gesetz (VÜPF) für sechs Monate aufbewahrt werden und dem IT-Sicherheitsbeauftragten der Informatikdienste zugänglich gemacht werden, sofern die Daten für eine Strafverfolgung durch Polizeiorgane benötigt werden.
9. Bei technischen Problemen kann der Technik-Verantwortliche logfiles beiziehen und auswerten um die Ursache zu klären. Eine personenbezogene Auswertung ist grundsätzlich untersagt.
10. Aufgezeichnete Randdaten sind als vertraulich zu betrachten und sollen mit geeigneten Massnahmen vor dem Zugriff durch Unberechtigte geschützt werden.
11. Inhalte von eMails Dritter dürfen nicht überprüft oder zur Kenntnis genommen werden.
12. Der Technik-Verantwortliche darf in seinem Verantwortungsbereich ein Scanning nach Verwundbarkeiten (port-scan oder weiterführende Techniken) durchführen mit dem Ziel, diese zu beseitigen.
13. Elektronische Datenträger, die nicht weiter verwendet werden, sind vor der Entsorgung sicher zu löschen.

14. Der Einsatz eines Passwort-Cracker Tools auf Geräten von Mitarbeitenden ist ohne deren ausdrückliches Einverständnis nicht gestattet.
15. Leitet Informationen der Informatikdienste über Störungen oder Wartungsarbeiten nach eigenem Ermessen an die Mitarbeitenden weiter.

3. Richtlinien und Weisungen

- Die aktuellen "Weisungen über die Benutzung der IT-Ressourcen an der Universität Bern
- Die aktuellen "Weisungen der Universitätsleitung über das Netzwerk der Universität Bern"
- Die aktuellen "Richtlinien für Einträge von Hostnamen im DNS
- Die aktuellen "Richtlinien zum Datenschutz im IT-Bereich"
- Die aktuellen "Richtlinien über Vergabe und Protokollierung von IP-Adressen"
- Die aktuellen "Richtlinien betreffend Massen-E-Mails, elektronischem Anschlagbrett und Adressen der Studierenden"

Weitere oder aktualisierte Dokumente finden sich in der Rechtssammlung unter http://www.rechtsdienst.unibe.ch/content/rechtssammlung/informatik/index_ger.html.

4. Kontaktstellen

- | | |
|----------------------|----------------------------------------------------------------------------------|
| • ID Helpdesk | Tel. 4999 / eMail helpdesk@id.unibe.ch |
| • ID Sicherheitsteam | Tel. 5455 / eMail security@id.unibe.ch |
| • ID Netzwerkteam | eMail netzwerk@id.unibe.ch |

Informatikdienste der Universität Bern
Bern, 28. Juli 2009