Netzbetriebs- und Managementkonzept
der Universität Paderborn

Stand November 2012
Inhalt

1. Verantwortung- und Zuständigkeitsverteilung ............................................. 4
   1.1. Planung ................................................................................................. 4
   1.2. Betrieb .................................................................................................. 4
       1.2.1. Verkabelungsinfrastruktur ............................................................. 4
       1.2.2. Netzwerkkomponenten ................................................................. 4
       1.2.3. Netzdienste ................................................................................... 5
       1.2.4. Verfügbarkeit der angebotenen zentralen Netzdienste .................. 5
       1.2.5. Verwaltung von IP-Adressen, Betrieb des Domain-Name-Service (DNS) ................................................................. 5
       1.2.6. DHCP ............................................................................................. 5
       1.2.7. Radius-Server ............................................................................... 5
       1.2.8. Sicherheitsdienste ......................................................................... 5
       1.2.9. Multicast ....................................................................................... 5
       1.2.10. Internet-Anschluss ....................................................................... 5
       1.2.11. Weitere Dienste ........................................................................... 5

2. Administration ................................................................................................. 6
   2.1. Adress- und Namensraum ..................................................................... 6
   2.2. Identitätsmanagement und Benutzeroberwartung ................................. 6
   2.3. IP-Geräte ............................................................................................. 6
   2.4. WLAN .................................................................................................. 6

3. Netzmanagement .............................................................................................. 6
   3.1. Dienstqualität ....................................................................................... 6
   3.2. Dienstgüte ............................................................................................. 6
       3.2.1. Verfügbarkeit ................................................................................ 6
       3.2.2. QoS .............................................................................................. 7
       3.2.3. Bandbreitenbegrenzungen ............................................................ 7
       3.2.4. Service-Level-Reporting ............................................................... 7
   3.3. Wartungskonzept für aktive Netzwerkkomponenten .............................. 7
   3.4. Management der passiven Komponenten (Facility Management) ........ 8
   3.5. Netzüberwachung und Management der aktiven Komponenten .......... 8
   3.6. Störungsmanagement .......................................................................... 9

4. Accounting ...................................................................................................... 9
   4.1. Nutzungsstatistiken zu Informations- und Planungszwecken ............... 9
   4.2. Nutzungsstatistiken zu Abrechnungszwecken ..................................... 9
   4.3. Datenschutz ......................................................................................... 9

5. Sicherheit im Netz ........................................................................................... 10
   5.1. Verantwortlichkeit und Organisation ................................................... 10
       5.1.1. Aufgaben und Verantwortlichkeiten der dezentralen Netzverantwortlichen .......................................................... 11
       5.1.2. Aufgaben und Verantwortlichkeiten der Servergruppe des IMT .................................................................. 11
   5.2. Physikalischer Zugriff auf Netzkomponenten ....................................... 11
       5.2.1. Zugriff auf Datenleitungen ............................................................ 11
       5.2.2. Zugriff auf Hardware-Komponenten .......................................... 11
   5.3. Redundanz- und USV-Konzept ............................................................... 12
   5.4. Administrativer Zugriff auf Netzkomponenten ..................................... 12
       5.4.1. Berechtigungskonzept ................................................................. 12
       5.4.2. Konzept für Konfigurationen, Updates und Teststellungen ........ 13
       5.4.3. Backup-Konzept ......................................................................... 13
       5.4.4. Monitoring-Konzept .................................................................... 13
   5.5. Maßnahmen zur Kontrolle von Datenströmen ..................................... 13
5.5.1. Nutzung von Subnetzen und VLANs ................................................................. 13
5.5.2. Access Control Lists (stateless packet screen; Paketfilter) .......................... 13
5.5.3. Firewall zwischen Uni-Netz und Internet ......................................................... 13
5.5.4. IDP / IPS ............................................................................................................ 14
5.5.5. Quality of Service (QoS) .................................................................................. 14
5.6. Sicherer Verkehr über unsichere Netze ............................................................... 14
5.7. Zugangskontrollregeln zum Netz ....................................................................... 14
  5.7.1. Regeln zu Konfiguration der Netzwerkdosen und Vergabe von IP-Adressen an
         Festnetzdosen .................................................................................................... 14
  5.7.2. Netzzugang zum WLAN .................................................................................. 15
6. Betriebs- und Nutzungsregelungen ..................................................................... 15
7. Anhang: Leitlinie zur Informationssicherheit der Universität Paderborn .......... 16
1. Verantwortung- und Zuständigkeitsverteilung


1.1. Planung

Beteiligt an der Netzausbauplanung sind die Fakultäten, die Betriebseinheiten, der Bau- und Liegenschaftsbetrieb NRW (BLB), das Dezernat 5 der Verwaltung und, federführend, das IMT. In Zusammenarbeit mit den Fakultäten und Instituten ermittelt das IMT den Bedarf und entwickelt eine Planung für die mittelfristige Entwicklung in quantitativer und qualitativer Hinsicht. Diese Planung ist Grundlage für die Umsetzung in konkrete Anträge, Bau- und Beschaffungsmaßnahmen, für die insbesondere auch die Verwaltung und der Bau- und Liegenschaftsbetrieb NRW im Rahmen ihrer Zuständigkeiten Verantwortung tragen. Durch geeignete Abstimmungsprozesse mit dem IMT wird sichergestellt, dass die Intentionen der Planung tatsächlich umgesetzt werden. Das IMT evaluiert in gemeinsamen Projekten mit anderen Bereichen der Universität regelmäßig innovative Netztechniken auf ihre Eignung für den hochschulweiten Einsatz.

1.2. Betrieb

Die grundsätzliche Zuständigkeit für den Betrieb des lokalen Netzes liegt beim IMT. Dabei gelten folgende Vereinbarungen:

1.2.1. Verkabelungsinfrastruktur

(Kabelwege, Verteilerräume, Primär-, Sekundär-, Tertiärverkabelung, Funkstrecken)

Der technische Betriebsdienst (TBD) des Dezernats 5 ist zuständig für die Bereitstellung und den Betrieb von Kabelwegen und Verteilerräumen. Alle Messungen, sofern diese nicht Bestandteil der Ersterstellung sind, die Beschaltung der Verteilerschränke samt zugehöriger Dokumentation und die Beseitigung von Störungen obliegen dem IMT. Der Betrieb der Verkabelungsinfrastruktur erfolgt in enger Abstimmung zwischen TBD und IMT.

1.2.2. Netzwerkkomponenten

(Switche, Router, Access Points)

1.2.3. **Netzdienste**
Das IMT betreibt das Netz der Universität Paderborn und zentrale Netzdienste für die Hochschule. Einige der im Folgenden aufgelisteten Netzdienste (DNS, DHCP, RADIUS) werden grundsätzlich vom IMT und nur in einigen wenigen Fällen auch dezentral erbracht. Ähnlich wie bei anderen Diensten (E-Mail, WWW, Datensicherung) erfolgt weiterhin eine Rezentralisierung in Kooperation zwischen IMT und den dezentralen Betriebsgruppen.

1.2.4. **Verfügbarkeit der angebotenen zentralen Netzdienste**

1.2.5. **Verwaltung von IP-Adressen, Betrieb des Domain-Name-Service (DNS)**

1.2.6. **DHCP**
Das IMT betreibt einen zentralen DHCP-Dienst für die gesamte Universität. Dieser Service wird teilweise auch von den Fakultäten für die ihnen zugeteilten IP-Bereiche selbst erbracht.

1.2.7. **Radius-Server**
Um eine einheitliche Authentifizierung der Nutzer beim Zugang zum WLAN und per Wählmodem sicherzustellen, betreibt das IMT einen redundant ausgelegten, zentralen Radiusserver.

1.2.8. **Sicherheitsdienste**
Die implementierten netzseitigen Sicherheitsmechanismen werden in Kapitel 5 genauer erläutert.

1.2.9. **Multicast**
Multicastfähigkeit ist flächendeckend erreicht.

1.2.10. **Internet-Anschluss**

1.2.11. **Weitere Dienste**
(E-Mail, WWW, Daten- und Speicherverwaltung, Videodienste, digitale Bibliothek, eLearning)

2. Administration

2.1. Adress- und Namensraum

Die Universität Paderborn verfügt über ein eigenes Class-B-Netz (131.234.0.0) sowie über 17 Class-C-Netze. Die Struktur des Namensraums unterhalb von uni-paderborn.de/upb.de folgt den Strukturen auf der Ebene der Fakultäten, Institute, Lehrstühle und Arbeitsgruppen.

2.2. Identitätsmanagement und Benutzerverwaltung

Das IMT hat gemeinsam mit der Verwaltung ein hochschulweites Identitätsmanagement aufgebaut und betreibt darauf basierend eine zentrale Benutzerverwaltung. Hochschulweite Dienste nutzen die zentralen Authentifizierungsdienste via LDAP, Active Directory und Kerberos.

2.3. IP-Geräte

Alle am Datennetz der Hochschule stationär betriebenen Geräte müssen bei einem Netzverantwortlichen oder beim IMT angemeldet werden. Bei der Anmeldung muss eine verantwortliche Person benannt werden, die bei Missbrauch oder Problemen mit dem Gerät kontaktiert werden kann. Das IMT trägt von gemeldeten Geräten die Hostnamen und IP-Adressen in die zentrale Hosttabelle ein.

2.4. WLAN

Um das WLAN der Universität Paderborn benutzen zu können, muss man als Benutzer registriert sein. Die Authentifizierung erfolgt im eduroam-Verbund des DFN-Vereins für lokale Benutzer mittels 802.1X und X.509-Zertifikat. Für die anderen SSIDs erfolgt eine webbasierte Authentifizierung mittels Benutzername und Passwort.

3. Netzmanagement

3.1. Dienstqualität

Das IMT berät die Angehörigen der Universität Paderborn bei der Nutzung der angebotenen Netzdienste, unterstützt bei der Aufklärung von Störungen und hält regelmäßige Informations- und Schulungsveranstaltungen ab. Für die Netzverantwortlichen der Universität Paderborn ist ein geschlossener Webbereich eingerichtet, in dem interne Detailinformationen zur Verfügung gestellt werden. Zusätzlich werden Informationen über eine Mailingliste weitergeleitet.

3.2. Dienstgüte

3.2.1. Verfügbarkeit

niedriger gehalten werden, da keine sehr kurzen und damit sehr teuren Reaktionszeiten vereinbart werden müssen.

3.2.2. QoS
Die Mehrheit der von IMT installierten aktiven Netzwerkkomponenten erfüllt bereits die Anforderungen an IP QoS. Im bisher reinen Datennetzwerk war der Bedarf an flächendeckender QoS-Installation nicht vorhanden. Durch die Einführung von Sprachdiensten (VoIP) in einigen Neubauten (Gebäude O, Gebäude ZM1) wurde, begrenzt auf diese Gebäude, die Bereitstellung garantiert der Netzleistung mittels QoS notwendig. Für die nächste Ausbaustufe des Netzes und die Migration auf VoIP ist die Evaluation und Umsetzung des flächendeckenden QoS geplant.

3.2.3. Bandbreitenbegrenzungen
Eine Bandbreitenbegrenzung ist an der Universität Paderborn nicht implementiert.

3.2.4. Service-Level-Reporting
Das IMT stellt in einem geschützten Webbereich den Netzverantwortlichen an der Universität die folgenden Informationen über den Zustand der Netzdienste zur Verfügung:

- Aktuelle Version der Konfiguration des zentralen IDS/IPD/Firewall-Systems
- IP-Filter für Subnetze
- Sicht auf den aktuellen Zustand des Netzes (Lese-Zugriff auf das Orion-Netzwerk-Management-System von SolarWinds) und Auslastungsstatistiken (Switche / Router)
- Die Host-Tabelle 131.234.0.0 der Universität Paderborn
- Liste der IP-Netze 131.234.0.0 und der zuständigen Betreuer
- Liste aller VLANs und Router zu den VLANs

3.3. Wartungskonzept für aktive Netzwerkkomponenten
Das IMT geht nicht davon aus, dass eine Komplettwartung des Hochschulnetzes durch einen externen Dienstbieter realisiert werden sollte. Einige wenige Dienste, die vom IMT nicht erbracht werden können, werden extern eingekauft.

Das Wartungskonzept des IMT beinhaltet:

- Redundante Auslegung der zentralen Netzleitungen und aktiven Netzwerkkomponenten (Kernnetz und Gebäude-Anbindung)
- Identifikation von Störungen, Störungsbehebung einschließlich Aus- und Einbau von Komponenten durch das IMT
- Einsatz möglichst einheitlicher Produktlinien, um eine homogene Netzinfrastuktur zu schaffen und dadurch Einarbeitungs- und Managementaufwand zu minimieren, eine einfache Austauschbarkeit der Geräte zu ermöglichen und eine hohe technische Kompetenz aufzubauen.
- Vorratshaltung einiger weniger Ersatzgeräte für meisteingesetzte Komponenten (Etageswitche)
• Servicewartungsvertrag für alle Netzwerkkomponenten (außer Etage) mit einem Servicepartner mit folgenden Leistungen:
  o Austausch defekter Komponenten aus dem Kernbereich innerhalb von 4 Stunden
  o Austausch defekter Teile aus dem sekundären Bereich innerhalb von 24 Stunden
  o Lizenzrechte für Softwareupdates
  o Third-Level-Support bei inhaltlichen Problemen (Telefon-, E-Mail-Support)

3.4. Management der passiven Komponenten (Facility Management)


Die Administration der beiden Systeme obliegt dem IMT.

3.5. Netzüberwachung und Management der aktiven Komponenten


Das Konfigurationsmanagement erfolgt im Wesentlichen manuell, unterstützt durch eigene Skripte. Die Wartung und der Betrieb dieser Vielzahl von Tools sind nicht effizient, die Funktionalität nicht ausreichend.

Angestrebt wird ein zentral installiertes, hardwareübergreifendes Netzwerk-Management-System, das auf standardisierte Protokolle und Schnittstellen zugreifen kann und folgende Funktionen realisiert:
  • Konfigurationsverwaltung und Steuerung des Netzwerkes
  • Unterstützung bei Planung, Erweiterung und Wartung des Netzwerkes
• Fehlermanagement, Aufdeckung von Engpässen im Netz und Lösungsvorschläge
• Performance-Management, Protokollierung, Steigerung der Netzeffizienz
• Report-, Event- und Benachrichtigungsfunktionen
• Verteilung von Netzwerk-Ressourcen QoS
• Energiemanagement

3.6. Störungsmanagement

Viele Geschäftsprozesse der Universität sowie die Arbeitsfähigkeit ihrer Angehörigen hängen wesentlich von der Funktionsfähigkeit des Netzes und der Netzdienste ab. Störungen werden durch Überwachungssysteme oder durch Meldungen der Nutzer erkannt. Fehlermeldungen können sowohl telefonisch an die Hotline des IMT (05251-605544) als auch per E-Mail an benutzerberatung@uni-paderborn.de gemeldet werden. Zur dokumentierten und nachhaltigen Verfolgung und Lösung von Problemen setzt das IMT das Open-Source-basierte Trouble-Ticket-System OTRS ein.


4. Accounting

4.1. Nutzungsstatistiken zu Informations- und Planungszwecken


4.2. Nutzungsstatistiken zu Abrechnungszwecken

Es werden keine Gebühren für die Nutzung des Netzes der Universität Paderborn berechnet.

4.3. Datenschutz

Im Zuständigkeitsbereich des IMT fallen Daten beim Betrieb des Netzes und der zentralen Server an. Es werden grundsätzlich nur die Daten gesammelt, die zur Erbringung der Netzwerkdienste erforderlich sind.

Dabei ist datenschutzrechtlich bei personenbezogenen Daten zwischen Bestands- und Verbindungsdaten zu unterscheiden:

• Bestandsdaten sind personenbezogene Daten wie Name, Adresse, Bankverbindung, die für ein Vertragsverhältnis notwendig sind bzw. in der Hochschule gespeichert werden, um eine Zuordnung zwischen Login-Namen und juristischen Personen sicherzustellen.
Verbindungsdaten beschreiben den Zugang und die Aktivitäten eines Nutzers (Benutzerkennungen, dynamisch vergebene IP-Adressen, Verbindungen, genutzte Dienste etc.). Häufig ist auch von Verbindungsdaten die Rede, wenn es spezieller darum geht, wer wann mit wem kommuniziert hat. Höchste datenschutzrechtliche Relevanz haben die Inhalte der Kommunikation.

Das IMT sammelt, speichert und wertet aktiv Verbindungsdaten aus, sofern sie für den ordnungsgemäßen Betrieb des Netzes oder der Server notwendig sind. Im IMT existiert eine Liste dieser Daten, in der der betriebliche Zweck und die daraus abgeleitete Dauer der Speicherung aufgelistet sind. Das IMT gibt Verbindungsdaten an auskunftssuchende Behörden nur nach Rücksprache mit dem Justiziarat der Universität Paderborn weiter, wenn die entsprechenden juristischen Grundlagen dafür vorhanden sind.

Bezüglich der Netzdienste werden aufgezeichnet:

- **Logdaten**

- **Personenbezogene Verbindungsdaten**

5. Sicherheit im Netz


Grundlegende Maßnahmen der Netz sicherheit werden sich vermutlich im Zuge der Weiterentwicklung der IT-Sicherheit an der Universität Paderborn ebenfalls ändern. An dieser Stelle wird daher der IST-Zustand ohne weitere Bewertung beschrieben.

5.1. Verantwortlichkeit und Organisation

5.1.1. Aufgaben und Verantwortlichkeiten der dezentralen Netzverantwortlichen


Die dezentralen Netzverantwortlichen sind verpflichtet,

- die definierten Workflows einzuhalten,
- an Netzwerk-Schulungen, die vom IMT gehalten werden, teilzunehmen. Die Schulungen werden veranstaltet, um die jeweils aktuellen Entwicklungen im Netzwerkbereich zu kommunizieren.

5.1.2. Aufgaben und Verantwortlichkeiten der Servergruppe des IMT


5.2. Physikalischer Zugriff auf Netzkomponenten

5.2.1. Zugriff auf Datenleitungen

Zugriff auf die passive Infrastruktur im Netz (Datenleitungen) haben die Mitarbeiter der Netzgruppe im IMT, die Mitarbeiter des TBD in Dez. 5 sowie auftragsorientiert externe Dienstleister nach vorheriger Absprache und Beauftragung durch Dez. 5 oder IMT.

5.2.2. Zugriff auf Hardware-Komponenten

Die Hardware-Komponenten (Router, Switches, Bridges, Controller, Server, AccessPoints, USV) im Netzbereich befinden sich in Netzwerkspeicher, in Serverräumen und in der Freifläche.

- Netzwerkverteilerräume
\begin{itemize}
\item \textbf{Serverräume}


\item \textbf{Freifläche}


5.3. \textbf{Redundanz- und USV-Konzept}

Zur Erhöhung der Verfügbarkeit werden wichtige Netzwerkkomponenten, soweit wirtschaftlich und technisch möglich, redundant ausgelegt. Dies betrifft das Kernnetz (die beiden Core-Router vertreten sich gegenseitig im Fall einer Störung), die Gebäudeanbindung (alle Gebäude sind über zwei Gebäuderouter, die jeweils an jedem der beiden Core-Switche angeschlossen sind, angebunden), die Außenanbindung (redundante Datenleitung zum Provider) als auch wichtige Netzdienste (Firewall, Loadbalancer, dhcp, dns, ntp und radius). Diese Komponenten sind zusätzlich auch durch USV-Anlagen abgesichert.

Switches auf den Etagen sind nicht redundant ausgelegt, jedoch jeweils redundant an beide Gebäuderouter angeschlossen und werden nur in einigen wenigen Fällen per USV abgesichert. Für die Etagenswitche hält das IMT Hardware zum kurzfristigen Ersatz auf Lager. Bei den WLAN-Controllern ist ein Controller mehr als notwendig im Einsatz. Durch die Überprovisionierung steigt zum einen die Performance, zum anderen die Verfügbarkeit, weil bei Ausfall eines Controllers die entsprechenden Access Points automatisiert von den übrigen bedient werden.

5.4. \textbf{Administrativer Zugriff auf Netzkomponenten}

5.4.1. \textbf{Berechtigungskonzept}

Der administrative Zugang zu den aktiven Netzkomponenten (Router, Switche, Controller) ist durch ein personenbezogenes sowie ein rechnerbezogenes Rollen- und Rechtekonzept realisiert.

Alle vom IMT gewarteten Netzwerkkomponenten liegen mit ihrem Management-Interface in einem besonders gesicherten VLAN. Der Zugang zum diesem VLAN wird mittels ACLs auf den zuständigen Routern eingeschränkt. Die Pflege der zugelassenen Rechner erfolgt durch die Leitung der IMT-Netzgruppe. Zusätzlich sind die zugelassenen Protokolle beschränkt. Es sind erlaubt:

\begin{itemize}
\item ssh und https für die Administration
\end{itemize}
Der eigentliche Zugang erfolgt durch eine persönliche Benutzerkennung und ein Passwort. Für die administrativen Zugriffsrechte wird in der Netzgruppe ein Admin-Passwort bekannt gegeben. Das Passwort wird regelmäßig gewechselt und ist für Notfälle im Notfall-Ordner hinterlegt.

5.4.2. Konzept für Konfigurationen, Updates und Teststellungen

5.4.3. Backup-Konzept
Die Konfiguration der Netzkomponenten wird per TFTP auf dem TFTP-Server isis.uni-paderborn.de regelmäßig gesichert und kann so im Notfall wiedereingespielt werden.

5.4.4. Monitoring-Konzept

5.5. Maßnahmen zur Kontrolle von Datenströmen
Die folgenden netzseitigen Sicherheitsmaßnahmen sind an der Universität Paderborn implementiert.

5.5.1. Nutzung von Subnetzen und VLANs

5.5.2. Access Control Lists (stateless packet screen; Paketfilter)
Zwischen Subnetzen wird zur Sicherung der Sicherheitsklassen mit ACLs gearbeitet. Die ACLs werden zentral auf dem TFTP-Server isis.uni-paderborn.de verwaltet und per TFTP auf die entsprechenden Router umverteilt und aktiviert. Die aktuellen Versionen der ACLs sind nur für die Netzverantwortlichen zu sehen unter imt.uni-paderborn/imtnet/acls.

5.5.3. Firewall zwischen Uni-Netz und Internet
Zwischen dem Internet und der Universität sind zwei redundant ausgelegte Firewall/Intrusion-Prevention-Systeme (Produkt Stonegate der Firma StoneSoft) implementiert. Die Geräte sind zwischen dem DFN-Intemetrouter und den Core-Routern der Universität angebunden und wer-

5.5.4. IDP / IPS

5.5.5. Quality of Service (QoS)
In einem Teilbereich des Netzes ist derzeit für die Sicherung von VoIP Quality of Service implementiert. Die implementierten Regeln sind unter https://wiki.uni-paderborn.de/QoS zu finden.


5.6. Sicherer Verkehr über unsichere Netze

Zur Sicherung der Vertraulichkeit der Daten wird an der Universität Paderborn unverschlüsselte Kommunikation wie TELNET oder FTP nicht unterstützt und vom IMT auch nicht angeboten. Es werden stattdessen Verfahren mit Verschlüsselung (ssh, scp, sftp) auch beim Zugriff auf den Mailserver via IMAP und POP oder beim Zugriff auf Webbereiche (https) eingesetzt.

5.7. Zugangskontrollregeln zum Netz
Der Netzzugang an der Universität Paderborn ist möglich über Festnetzdosen in Räumen, Festnetzdosen in Freiflächen (so genannte Grüne Dosen) und das WLAN. Grundsätzlich ist eine anonyme Nutzung des Netzes nicht möglich.


5.7.1. Regeln zu Konfiguration der Netzwerkdosen und Vergabe von IP-Adressen an Festnetzdosen

- Dosen in Büros und in Räumen mit einem begrenzten physikalischen Zugang (Schlüssel, Zugangskarte), an den stationäre oder mobile Rechner angeschlossen sind (AG-Pools, Labore)

Die Dosen werden nur auf Antrag eines Netzverantwortlichen für ein gewünschtes VLAN freigeschaltet, die IP-Vergabe erfolgt durch eine Eintragung im DNS oder per
DHCP mit fester Zuordnung MAC-Adresse zu IP. An die Dosen dürfen beliebige Rechner angeschlossen werden oder nach Wunsch nur ein durch MAC-Adresse bekannter Rechner (PortSecurity). Zusätzlich können die Netzverantwortlichen VLANs, für die sie verantwortlich sind, nur in Räumen der eigenen Bereiche nach Bedarf mit Hilfe einer Benutzeroberfläche mandantengesteuert selbst schalten.

- **Dosen in frei zugänglichen Räumen, an die stationäre Rechner angeschlossen sind (Pools, Labore)**

Eine Dose wird nur auf Antrag eines Netzverantwortlichen für ein gewünschtes VLAN freigeschaltet, die IP-Vergabe erfolgt durch eine Eintragung im DNS oder per DHCP mit fester Zuordnung MAC-Adresse zu IP. An der Dose darf nur ein durch die MAC-Adresse bekannter Rechner (PortSecurity) angeschlossen werden. Auch hier haben die Netzverantwortlichen die Möglichkeit, selbst Anschlüsse wie oben beschrieben zu schalten.

- **Dosen in frei zugänglichen Räumen/Flächen für mobile Rechner (Grüne Dosen)**

Die Dosen werden vom IMT in ein bestimmtes, gesichertes VLAN geschaltet. Die IP-Vergabe erfolgt ohne feste Zuordnung per DHCP. Zugang zum Netz ist nur mit VPN (OpenVPN) möglich.

**5.7.2. Netzzugang zum WLAN**

Für den produktiven Einsatz existieren an der Universität Paderborn die SSIDs eduroam, webauth und upb_tmp. Für alle SSIDs erfolgt die Vergabe der IP-Adressen per DHCP ohne feste Zuordnung zum Nutzer oder der Mac-Adresse seines Rechners.

- **Webauth und upb_tmp**


- **Eduroam**


**6. Betriebs- und Nutzungsregelungen**

- Verwaltungsordnung (siehe http://imt.uni-paderborn.de/verwaltungsordnung/)
7. Anhang : Leitlinie zur Informationssicherheit der Universität Paderborn

PRÄAMBEL


ZIELE UND ADRESSATENKREIS
Diese Leitlinie regelt die Verantwortung und die Zuständigkeiten sowie die Zusammenarbeit im hochschulweiten IT-Sicherheitsprozess. Es ist ihr Ziel nicht nur die existierenden gesetzlichen Auflagen zu erfüllen, sondern auch die in der Hochschule verarbeiteten, übertragenen und gespeicherten Daten und Anwendungen vor Missbrauch zu schützen. Sie ist an alle Organisationseinheiten, Mitglieder und Angehörige der Universität Paderborn sowie an Dritte gerichtet, die IT-Systeme und IT-Verfahren benutzen oder betreiben.

LEITSÄTZE

Als zusätzliche Prinzipien der Informationssicherheit sind für die Universität Paderborn festgelegt

- **Wohlorganisierung**: Für alle IT-Systeme und IT-Verfahren gibt es klare Verantwortlichkeiten

- **Informiertheit**: Alle Anwenderinnen und Anwender von IT-Systemen und IT-Verfahren sollen sich der für sie wesentlichen Sicherheitsrisiken und deren Abwehrmaßnahmen bewusst sein.
• **Zurechenbarkeit:** Jede von vernetzten Rechnern der Universität Paderborn ausgehende Aktivität soll einer Person zugeordnet werden können.

• **Aktualität:** Die eingesetzten IT-Systeme und IT-Verfahren sollen den jeweils aktuellen Sicherheitsempfehlungen einschlägiger Institutionen entsprechen.

• **Angemessenheit:** Alle Maßnahmen sind mit Augenmaß und in Hinblick auf die Gefährdungen und Risiken sowie ihr Kosten-Nutzen-Verhältnis zu wählen.

• **Wahrung eines permanenten Regelkreislaufes:** Die Wirksamkeit und Angemessenheit der Sicherheitsmaßnahmen wird regelmäßig überprüft. Verletzungen der Informationssicherheit werden kommuniziert und dokumentiert.

• **Recht auf informationelle Selbstbestimmung:** Die Universität unterstützt aktiv das Recht auf informationelle Selbstbestimmung und ist bestrebt die Erhebung, Speicherung und Nutzung personenbezogener Daten auf das Notwendige zu beschränken (Minimalität).

**VERANTWORTLICHKEITEN**

Die Leitung der Universität trägt die Gesamtverantwortung für die Informationssicherheit an der Universität Paderborn. Diese wird fachlich durch den Lenkungskreis für Informationssicherheit (LIS) wahrgenommen.

Die Verantwortung für die IT-Sicherheit jeder Organisationseinheit oder Einrichtung liegt bei der jeweiligen Leitung. Sie kann fachlich durch einen IT-Verantwortlichen wahrgenommen werden.

Falls externe Dienstleister beauftragt werden sind diese bei Aufnahme einer Vertragsbeziehung über entsprechende Passagen im Regelwerk zur Informationssicherheit zu informieren und schriftlich auf dessen Einhaltung zu verpflichten.

Alle Anwenderinnen und Anwender tragen die Verantwortung, bestimmungsgemäß und sachgerecht mit den von ihnen genutzten IT-Systemen, IT-Verfahren und Informationen umzugehen.


**ORGANISATIONSSTRUKTUR**

Zur Gestaltung des Informationssicherheitsprozesses an der Universität Paderborn wird die im Folgenden beschriebene Organisationsstruktur festgelegt. Sie besteht aus dem Lenkungskreis für Informationssicherheit, dem IT-Sicherheitsbeauftragten sowie den IT-Verantwortlichen und dem Computer Notfallteam.

**Lenkungskreis für Informationssicherheit (LIS)**

Der Lenkungskreis für Informationssicherheit (LIS) steuert im Auftrag des Präsidiums den IT-Sicherheitsprozess an der Universität Paderborn. Er erarbeitet und empfiehlt in Zusammenarbeit mit den Verantwortlichen im Bereich Informationssicherheit strategische Empfehlungen und Maßnahmen wie diese Leitlinie und das Regelwerk zur Informationssicherheit und überprüft ihre Umsetzung.

Er berät das Präsidium im Bereich Informationssicherheit und empfiehlt und verantwortet hochschulweite Projekte in diesem Bereich.
Er nimmt die jährlichen Berichte der IT-Verantwortlichen im Bereich Informationssicherheit entgegen und berichtet einmal jährlich dem Präsidium zum Stand der Umsetzung der Informationssicherheit an der Universität Paderborn.
Er wählt aus seiner Mitte einen Ansprechpartner für Informationssicherheit, den IT-Sicherheitsbeauftragten der Universität Paderborn.

Zum Lenkungskreis zählen
- der CIO oder ein anderer Beauftragter oder eine Beauftragte des Präsidiums
- die/der behördliche Datenschutzbeauftragte
- jeweils eine Vertreterin oder ein Vertreter der Personalräte
- jeweils eine Vertreterin oder ein Vertreter der zentralen Organisationseinheiten, die hochschulweite IT-Systeme und IT-Verfahren verantworten, derzeit die Universitätsverwaltung, die Universitätsbibliothek, das Zentrum für Informations- und Medientechnologien (IMT)
- eine vom Präsidium benannte fachkundige Wissenschaftlerin oder ein vom Präsidium benannter fachkundiger Wissenschaftler
- die IT-Verantwortlichen der Fakultäten
- eine fachkundige Vertreterin oder ein fachkundiger Vertreter aus der Studierendenschaft (nach der Einführungsphase)

Das Präsidium sowie der LIS können weitere Teilnehmende zur Beratung hinzuziehen.

**IT-Sicherheitsbeauftragter der Universität**

Die/Der IT-Sicherheitsbeauftragte ist die zentrale Ansprechperson zu Fragen der Informationssicherheit an der Universität Paderborn.
Sie/Er koordiniert die Umsetzung der vom LIS empfohlenen Maßnahmen und verantwortet die Weiterentwicklung und Veröffentlichung des Regelwerks für Informationssicherheit.
Sie/Er berät die Organisationseinheiten, die Datenschutzbeauftragte oder den Datenschutzbeauftragten und organisiert Schulungs- und Sensibilisierungsmaßnahmen.

**IT-Verantwortliche**

Die IT-Verantwortlichen sind zugleich Ansprechpartner für Informationssicherheit und tragen Sorge für die Weiterentwicklung von Maßnahmen sowie die Umsetzung der im IT-Sicherheitsprozess erarbeiteten Vorgaben. Sie informieren und berichten dem IT-Sicherheitsbeauftragten über Sicherheitsvorfälle in ihrem Verantwortungsbereich. Vorfälle mit Bezug auf personenbezogene Daten sind unverzüglich und unmittelbar dem IT-Sicherheitsbeauftragten anzuzeigen.
Computer Notfallteam


REGELWERK ZUR INFORMATIONSSICHERHEIT