Hochschule für Technik und Wirtschaft Berlin
Fachbereich 2 – Ingenieurwissenschaften Technik und Leben
Dekan des Fachbereichs 2

Hochschule für Technik
und Wirtschaft Berlin
University of Applied Sciences

Richtlinie für die Organisation und den Betrieb der IT-Infrastruktur des Fachbereichs 2 der HTW Berlin (IT-Richtlinie des FB 2)

(beschlossen vom Fachbereichsrat des FB 2 am 10. Oktober 2018)

1 Zielsetzung

Der Fachbereich 2 sieht es als strategisches Ziel an, eine sehr gut ausgebaute, moderne und insgesamt leistungsfähige IT-Infrastruktur für Lehre und Forschung bereit zu stellen. Diese Infrastrukturseite soll durch hervorragenden Service den Studierenden, Professoren und dem wissenschaftlichen und sonstigen Personal leicht zugänglich gemacht und funktionsfähig erhalten werden.

Um neuen Anforderungen gerecht zu werden, entwickeln und betreiben die IT-Querschnittsdienste und die IT-Laboringenieure des FB 2 adäquate IT-Lösungen. Dies passiert in enger Abstimmung und ggfs. Zusammenarbeit mit dem Hochschulrechenzentrum (HRZ).

Für diese Aktivitäten regelt die hier vorliegende IT-Richtlinie des FB 2 die Rahmenbedingungen entsprechend den für IT-Systeme an der HTW Berlin geltenden Grundsätzen der Absicherung der Vertraulichkeit, Integrität und Verfügbarkeit der IT-Systeme mit dem Ziel der Etablierung des IT-Grundschutzes.

Darüber hinaus spezifiziert die IT-Richtlinie des FB 2 organisatorische und technische Regelungen, die für die Umsetzung der allgemeinen IT-Richtlinien der HTW und für die Etablierung des IT-Grundschutzes notwendig sind:

- Hard- und Softwarekonzept für den IT-Betrieb
- Datensicherungskonzept
- Patch- und Änderungsmanagement
- Notfall- und Vertretungskonzept
- Benutzer- und Berechtigungsverwaltung
- Supportkonzept
- Absicherung des berechtigten Zugangs und Zutritts
- Konzept zur Sicherung vor Schadprogrammen

Die vorliegende Richtlinie wird dauerhaft fortgeschrieben.

2 Geltungsbereich und Umfang der angebotenen IT-Leistungen

Die in dieser Richtlinie zusammengefassten Regelungen gelten für die vom FB 2 betriebene IT-Infrastruktur für Lehre und Forschung (hierunter fällt auch im HRZ gehostete FB2-Hardware).

Abgrenzung:

Ausdrücklich ausgenommen von den Regelungen dieser Richtlinie sind sämtliche Bereiche, deren Umsetzung in Verantwortung des HRZ bereits geregelt sind, so z. B. die IT-Infrastruktur der Mitarbeiter der FB 2 Verwaltung, die vom HRZ betrieben wird.

Im Einzelnen umfassen die von in dieser Richtlinie erfassten Leistungen der FB 2 IT-Services aktuell folgende Punkte:

- Betrieb, Pflege und Wartung von IT-Laboren für die Lehre inklusive benötigter Infrastruktur (Hardware und Software)
- Betrieb, Pflege und Wartung von Serveranwendungen für Lehr- und Forschungsprojekte (soweit nicht explizit anders geregelt) sowie Gewährleistung einer angemessenen Verfügbarkeit für diese Anwendungen
- Betrieb, Pflege und Wartung von Querschnittsdiensten (Virenscanner, Backup, Speicherplatzbereitstellung, Softwareverteilung, Plotterdienste, etc.)
- Gewährleistung eines Grundschutzes an IT-Sicherheit in Bezug auf den IT-Laborbetrieb und die vom FB2 betriebenen Server sowie ggfs. Rechnern von Professoren und wissenschaftlichen Mitarbeitern. Für Rechner von Professoren und wissenschaftlichen Mitarbeitern wird eine IT-Grundschutz konforme Konfiguration angeboten.
- Vorbereitung der Beschaffung, Erstinstallation und Wartung der Dienstrechner von Professoren und wissenschaftlichen Mitarbeitern, sofern diese IT-Grundschutz konform konfiguriert werden sollen bzw. sind
- Beratung und Vorbereitung für IT-bezogene Beschaffungsvorgänge für Labor-IT und IT-Querschnitt
- Betreuung studentischer Arbeitsgruppen und Lehrveranstaltungen in den IT-Laboren in Bezug auf die Nutzbarkeit der Infrastruktur und ausgewählter Spezial- oder Fachsoftware

3 Referenzierte Richtlinien der HTW Berlin

Neben den in der vorliegenden Richtlinie gemachten Aussagen gelten grundsätzlich die geltenden gesetzlichen Bestimmungen, ergänzt durch die jeweils aktuellen Ordnungen und Richtlinien der HTW Berlin. Unter den letzten Punkt fallen insbesondere folgende Dokumente:

- Benutzungsordnung Informationsverarbeitungsinfrastruktur der HTW Berlin
- Richtlinie Informationssicherheitsmanagement der HTW Berlin (ISM-Richtlinie)
- Richtlinie für die Gewährung der Informationssicherheit der HTW Berlin (IS-Richtlinie)

Diese Dokumente unterliegen einer kontinuierlichen Weiterentwicklung. Deshalb wird dabei allein auf die Dokumententitel und nicht auf Versionen verwiesen.

4 Organisationskonzept und -struktur der IT des FB 2

Die IT des FB 2 gliedert sich in die Bereiche IT-Betrieb, IT-Querschnitt und IT-Sicherheit.

Die IT im Fachbereich wird koordiniert vom **IT-Board** des FB2, das aus dem **Dekan**, dem **Leiter des IT-Querschnitts**, dem **IT-Laborleiter** und dem **dezentralen IT-Sicherheitsbeauftragten** besteht.

Der Dekan übernimmt für den FB die Rolle des Chief Informationen Officers (CIO) und gewährleistet über den Fachbereich die Sicherstellung eines finanziellen Budgets für den ordnungsgemäßen Betrieb der IT-Systeme in den IT-Pools (IT-Betrieb) und der IT-Infrastruktur des FB2 (Querschnittsdienste). Er übernimmt als CIO die fachliche Verantwortung für den Betrieb der IT-Querschnittsdienste und deren technische Ausstattung. Er ist Fachvorgesetzter für die dem IT-Querschnitt zugeordneten IT-Mitarbeitern. Die Aufgabe und Funktionen für die IT-Querschnittsdienste kann der CIO professoral delegieren.

Der IT-Laborleiter übernimmt die fachliche Verantwortung für den Betrieb der IT-Labore und deren technische Ausstattung. Er ist Fachvorgesetzter für die IT-Labormitarbeiter, die dem IT-Betrieb zugeordnet sind.

Der dezentrale IT-Sicherheitsbeauftragte sorgt für den IT-Grundschutz und verfolgt alle IT-Sicherheitsrelevanten Aspekte des Fachbereichs. Er ist Fachvorgesetzter für die IT-Labormitarbeiter, die dem Bereich IT-Sicherheit zugeordnet sind (IT-Sicherheitsingenieure). Er kann in Abstimmung mit dem IT-Board auch eine Abschaltung von Teilen der IT-Infrastruktur vorschlagen. Die Abschaltung wird im IT Board beschlossen und durch den Dekan des FB2 angewiesen. In sehr dringlichen Fällen kann der IT-Sicherheitsbeauftragte Teile der IT-Infrastruktur auch temporär sofort abschalten.

Das IT-Board verteilt zu Beginn jedes Haushaltsjahres das zur Verfügung stehende Budget in die Bereiche IT-Betrieb, IT-Querschnitt und IT-Sicherheit, die dann eigenständig von den Bereichen verwaltet werden. Dies beinhaltet ebenfalls die SHK-Kapazitäten, die für die Bewirtschaftung eingesetzt werden.

Der Fachbereich verfolgt ein autonomes Verantwortlichkeitskonzept im IT-Bereich. Die IT-Laboringenieure und IT-Sicherheitsingenieure organisieren ihre Arbeitsaufgaben als Team unter der Maßgabe, dass es jeweils zwei Verantwortliche für die o. a. Aufgaben gibt, einen Hauptverantwortlichen und einen Stellvertreter, in dem Maße, wie es die Personalausstattung gestattet. Die operative Kontrolle des IT-Betriebes erfolgt durch den IT-Laborleiter. Die fachliche Ausrichtung der Laborbereiche auf die jeweiligen Studiengänge des Fachbereichs wird mit den Studiengangsprechern der Studiengänge koordiniert.

Die IT-Laboringenieure tragen entsprechend ihren Arbeitsaufgaben Verantwortung für einen oder mehrere der im folgenden beschriebenen Bereiche:

- Komplexlabor II/UI/BUI/LSE (IT-Betrieb)
- Komplexlabor BI und FM (IT-Betrieb)
- Komplexlabor FZT und MB (IT-Betrieb)

- IT-Querschnittsdienst (Fachbereich)
- IT-Sicherheit (Fachbereich)

5 Organisatorische und technische Regelungen für die IT des FB 2

In den organisatorischen und technischen Regelungen für die IT des FB 2 sind grundsätzliche Aussagen

- zum Hardware- und Softwarekonzept für den IT-Betrieb,
- zum Patch- und Änderungsmanagement,
- zum Sicherungskonzept (Backup/Restore/ggf. Archivierung),
- zum Notfall- und Vertretungskonzept,
- zur Benutzer- und Berechtigungsverwaltung,
- zum Supportkonzept (beteiligte Partner),
- zur Absicherung der Kontrolle von Zugang und Zutritt und
- zum Schutz vor Schadprogrammen

zu dokumentieren. Dabei müssen die angewandten Verfahren und formalen Regularien transparent gemacht werden. In jedem Fall muss die Nachhaltigkeit einer IT-Lösung deutlich nachgewiesen werden können.

5.1 Hard- und Softwarekonzept für den IT-Betrieb

Für den Betrieb der IT-Infrastruktur des FB 2 werden folgende Maßgaben empfohlen:

- In allen von dieser Richtlinie erfassten Bereichen der IT-Infrastruktur des FB ist eine IT-Grundschutz konforme Konfiguration anzustreben.
- Die Softwareverteilung für gängige Softwareprodukte in den IT-Laboren des FB 2 sollte zentral vorgenommen werden (vgl. auch Abschnitt Patch- und Änderungsmanagement).
- Die Serveranwendungen für Lehr- und Forschungsprojekte sollten in den vom FB 2 betriebenen Virtualisierungsumgebungen deployed werden.

5.2 Patch- und Änderungsmanagement

Für die IT-Labore des FB 2 gelten folgende Regelungen:

- Microsoft Updates werden über den WSUS-Server verteilt. Dabei werden Updates aus der Kategorie Sicherheitsupdates automatisch sofort genehmigt, Updates aus anderen Kategorien werden mit einer 11-tägigen Verzögerung genehmigt. Somit soll sichergestellt werden, dass alle sicherheitsrelevanten Updates sofort zur Wirkung kommen, aber vermieden werden, dass unzureichend getestete Updates aus anderen Kategorien unvorhergesehene Problem verursachen.

- Programmspezifische Updates werden über die KACE Softwareverteilung verteilt. Der FB2 hat über einen Subscriptionvertrag mit Quest die Möglichkeit auf Patches für gängige Softwareprodukte über die Kace zuzugreifen und diese zu verwenden. Die PCs der IT-Labore und LSE werden montags und donnerstags geprüft, und es wird nach neuen Patches der eingebundenen Softwareprodukte geprüft. Die Patchverteilung wird nach Softwareprodukt, Studiengang und möglichen Zeitfenstern außerhalb der Lehre durchgeführt. Mitarbeiter der Querschnittsdienste des FB 2 werden über den Stand der Patchverteilung via E-Mail informiert.

5.3 Datensicherungskonzept

Alle Netzlaufwerke werden täglich auf einem zweiten Server gespeichert. Die VM`s sind vollständig auf der NetApp gespeichert; diese Sicherung wird durch das HRZ verwirklicht.
Für das Backup der Cluster Nodes Server des FB 2 wird die Windows interne Sicherungssoftware verwendet. Hierbei wird ein tägliches Bare-Metal Backup erstellt. Zur Sicherung der verwendeten Volumes, welche über ein Storage System (Raid 10) bereitgestellt werden, wird die Software Acronis Backup Server verwendet. Diese sichert nach einem festgelegten Plan die einzelnen Volumes und repliziert die Sicherungen im Anschluss auf einem zweiten Backup Server, welcher physisch vom ersten Backupserver getrennt verwaltet wird. Mitarbeiter der Querschnittsdienste des FB 2 werden über den Stand der Sicherungen via E-Mail informiert.

5.4 Notfall- und Vertretungskonzept

Es existiert ein Notfallplan, der beschreibt, welche Server in welcher Reihenfolge gestartet werden muss. Dieser Plan ist für alle Administratoren der IT-Querschnittsdienste zugänglich. Da er sich neben anderen benötigten Informationen auf einem Netzlaufwerk befindet, gibt es ein Emergency Control Center (ECC), auf dem täglich alle Informationen lokal gespeichert werden, so dass bei einem Ausfall des Netzwerkes darauf zugriffen werden kann.
Für die Kommunikation mit den FB 2-Servern ist ein speziell konfigurierter Browser vorhanden.

Damit jedes System auch bei Ausfall eines Mitarbeiters administriert werden kann, sind für jedes System zwei Mitarbeiter verantwortlich.

5.5 Benutzer- und Berechtigungsverwaltung

Die Benutzerauthentifizierung erfolgt grundsätzlich über die HTW-weiten Accounts, die über das HRZ bereitgestellt und verwaltet werden. Der Zugang zu bestimmten Ressourcen erfolgt über die vom HRZ gepflegten Gruppen. In Fällen, in denen die Gruppen des HRZ nicht feingranular genug sind, werden Gruppen in der FB 2-Domäne erstellt und diesen Gruppen Accounts zugeordnet.

Werden für bestimmte Zwecke, z. B. im Rahmen von Forschungsprojekten, Root-Rechte auf einem System benötigt, wird nach Abgabe der unterschriebenen Nutzungsvereinbarung auf diesem System der HRZ Account als lokaler Administrator hinzugefügt. Ausnahmen bilden kurzlebige Linux VM's, bei denen sich der Aufwand der AD-Verknüpfung nicht lohnen würde. Bei diesen Maschinen wird eine Root-Konto mit RSA-Key für QS-Admins angelegt und ein weiteres Konto mit Root-Rechten für den Unterzeichner der Nutzungsvereinbarung.

5.6 Supportkonzept

Der Support von **Softwareanwendungen** ist für die IT-Hardware des FB 2 folgendermaßen geregelt:

- Für vom HRZ bereitgestellte Anwendungen (z.B. Webmail, LSF, Moodle, VPN u.a.) ist der zentrale IT-Support zuständig.
- Für zentral von den Querschnittsdiensten des FB2 bereitgestellte Anwendungen (z. B. gitlab, VersionOne, Wordpress-Instanzen) und virtuelle Maschinen für Projekte ist der FB2 Helpdesk zu kontaktieren.
- Für Standardanwendungen und Fachanwendungen in den IT-Laboren ist ebenfalls der FB 2- Helpdesk zu verwenden.
- Für jede Fachanwendung gibt es jeweils einen IT-Laboringenieur, der für den Support verantwortlich ist.

Bei Problemen mit dem Drucken und Scannen auf FB 2-Hardware ist ebenfalls der FB 2-Helpdesk zu kontaktieren.

5.7 Absicherung der Kontrolle von Zugang und Zutritt

Die IS-Richtlinie der HTW Berlin beschreibt die Grundsätze für den Zutritt zu den Räumlichkeiten bzw. der Zugang zu den IT-Diensten. Die Bedingungen für die Erlangung von Schlüsselberechtigungen sind in der „Schlüsselordnung" der HTW Berlin geregelt.

Für die Absicherung des Zugangs zu **Räumlichkeiten des FB 2** zeichnet das Dekanat federführend durch den Dekanatsgeschäftsführer verantwortlich.

5.8 Schutz vor Schadprogrammen

Bislang wird der Schutz vor Schadsoftware auf allen IT-Laborrechnern durch McAfee realisiert.
Diese Lösung soll durch den FortiClient von FortiNet abgelöst werden. Eine einheitliche Firewall-Lösung ebenfalls von FortiNet wird gerade durch das HRZ vorbereitet.

6 Behandlung von IT-Sicherheitsvorfällen der IT des FB 2

Entsprechend der IS-Richtlinie der HTW Berlin wird als **IT-Sicherheitsvorfall** ein Ereignis bezeichnet, bei dem ein Schaden hinsichtlich der Vertraulichkeit oder Integrität von Daten, oder/und der Verfügbarkeit von IT-Systemen aufgetreten ist. Einige typische Beispiele für IT-Sicherheitsvorfälle sind:

- Auftreten von Schadsoftware (z.B. Viren oder Trojaner)
- Hacking von z.B. Internet-Servern
- Fehlkonfigurationen an IT-Systemen, die zur Offenlegung von vertraulichen Daten oder/und zum Verlust von Daten führen
- Auftreten von Sicherheitslücken in Hard- oder Softwarekomponenten
- weitere kriminelle Handlungen, wie Einbruch, Diebstahl oder Erpressung mit IT-Bezug

Entsprechend der IS-Richtlinie sind bei Sicherheitsvorfällen an der IT-Infrastruktur des FB 2 für Lehre und Forschung folgende **Verhaltensregeln** und **Informationspflichten** einzuhalten:

- Im Bereich der **IT-Labore**: Sobald ein Fehler oder ein anderes Problem auftritt, ist umgehend der IT-Laboringenieur zu benachrichtigen. Der IT-Laboringenieur übernimmt die weitere Behandlung des IT-Sicherheitsvorfalls und meldet diesen an den dezentralen IT-Sicherheitsbeauftragten.

- **Lehr**- und **Forschungsprojekte** sowie **Professorenrechner**: Sobald ein Fehler oder ein anderes Problem auftritt, ist umgehend der IT-Querschnitt zu benachrichtigen. Der IT-Querschnitt übernimmt die weitere Behandlung des IT-Sicherheitsvorfalls und meldet diesen an den dezentralen IT-Sicherheitsbeauftragten.

- Der dezentrale IT-Sicherheitsbeauftragte dokumentiert und meldet den IT-Sicherheitsvorfall auf dem dafür vorgesehene Meldeweg und wertet diesen später aus.

- Im Umgang mit Sicherheitsvorfällen sind Ehrlichkeit und Kooperationsbereitschaft besonders wichtig. Die Meldung von Sicherheitsvorfällen wird daher immer positiv gewertet.

Hiervon abzugrenzen ist ein **Informationssicherheitsvorfall** mit **Datenschutzrelevanz**, d. h. ein Sicherheitsvorfall, bei dem personenbezogene Daten betroffen sind. Bei solchen Vorfällen ist in jedem Falle der zentrale Datenschutzbeauftragte der HTW Berlin einzubeziehen.

7 Datenschutz

Der Schutz personenbezogener Daten ist ein wichtiges Anliegen aller Mitarbeiter des Fachbereichs. Grundsätzlich erfolgt die Verarbeitung personenbezogener Daten im FB 2 nur zu dem Zweck, zu dem sie ursprünglich erhoben wurden und nur nach den Vorgaben der relevanten datenschutzrechtlichen Bestimmungen, insbesondere der Datenschutzgrundverordnung (EU-DSVGO) und des Bundesdatenschutzgesetzes.

Schon vor der IT-gestützten Datenverarbeitung (aber auch während dieser) werden technische und organisatorische Maßnahmen getroffen, die einen angemessenen Schutz für die personenbezogenen Daten bieten und eine den Anforderungen der EU-DSGVO entsprechende Verarbeitung sicherstellen. Dabei hängt die Auswahl der jeweiligen Maßnahmen vom Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie von den mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten der betroffenen Personen ab. Welche Maßnahmen als angemessen gelten, hängt zudem von der Eintrittswahrschein-lichkeit einer Datenschutzverletzung ab und muss jeweils im Einzelfall unter Berücksichtigung der Verhältnismäßigkeit beurteilt werden.

Alle Mitarbeiter des Fachbereichs bekennen sich zur Anwendung der folgenden handlungsleitenden Prinzipien zum Schutz personenbezogener Daten:

- Grundsatz der Datenvermeidung und Datensparsamkeit (Es werden nur die Daten erhoben, die nötig und zulässig sind, kein Bevorraten mit Daten.)

- Grundsatz der Zweckbindung (D. h., Daten dürfen nur für einen definierten Zweck verarbeitet werden. Pauschale Einverständniserklärungen sind ungültig).)

- Grundsätzliches Verbot mit Erlaubnisvorbehalt (Jede Verarbeitung personenbezogener Daten bedarf entweder der ausdrücklichen Einwilligung, die jederzeit widerrufen werden kann, oder einer gültigen Rechtsvorschrift.)

- Grundsätze der Verhältnismäßigkeit, der Bestimmtheit und Normenklarheit, der organisatorischen und verfahrensrechtlichen Absicherungen

gez.
Prof. Dr. Volker Wohlgemuth
Dekan des FB 2