Hochschule
für nachhaltige Entwicklung
Eberswalde

Amtliche Mitteilung

25.08.2016 | Nr. 192

Inhalt

Leitlinie zur Informationssicherheit

HNEE

Herausgeber: Der Präsident der Hochschule für nachhaltige Entwicklung Eberswalde
Haus- und Postanschrift: Hochschule für nachhaltige Entwicklung Eberswalde | Schicklerstraße 5 | 16225 Eberswalde

Leitlinie zur Informationssicherheit

1 Stellenwert der Informationsverarbeitung

Informationsverarbeitung und speziell die Informations- und Kommunikationstechnik sind von zentraler Bedeutung für die Aufgabenerfüllung der Hochschulen und Forschungseinrichtungen. Sie finden in allen Hochschulprozessen statt. IT-Anwendungen bilden inzwischen die Grundlage für die meisten Prozesse. Das Spektrum der IT-Anwendungen umfasst die rechnergestützte Informationsverarbeitung für Forschung, Lehre und Verwaltung sowie die Kommunikation mit externen Partnern und Auftraggebern.

Die Bedeutung der Informationstechnik in Forschung, Lehre und Verwaltung ist unterschiedlich hoch. Dementsprechend haben Störungen oder Ausfälle Auswirkungen unterschiedlicher Tragweite.
Die Hochschulleitung erkennt, dass sich die Risiken und die zu erwartenden Auswirkungen bei der Informationsverarbeitung verändern und für die Hochschule eine Existenzbedrohung annehmen können.

Mit der Leitlinie unterstreicht die Hochschulleitung die Bedeutung der Informationssicherheit für die Hochschule und bestätigt die Übernahme der Gesamtverantwortung für den Informationssicherheitsprozess.

Die Leitlinie zur Informationssicherheit ist Bestandteil eines abgestuften Regelwerks und bildet die Grundlage für die Erstellung weiterer fachspezifischer Richtlinien, Informationssicherheitskonzepte sowie Regelungen und Dienstanweisungen zur Informationssicherheit. Dabei gilt es auch, die Einhaltung aller gesetzlichen und vertraglichen Vorschriften bzgl. der Informationssicherheit und des Datenschutzes sicherzustellen.

2 Geltungsbereich

Diese Leitlinie ist verbindlich für sämtliche Hochschulmitglieder und Hochschulangehörige sowie alle organisatorischen Einheiten der Hochschule; es umfasst sämtliche Geschäftsprozesse aus Lehre, Forschung und Verwaltung.

Alle Mitglieder und Angehörigen der Hochschule sind verpflichtet, an der Umsetzung der Informationssicherheitsleitlinie kooperativ und verantwortungsbewusst mitzuwirken.
Die Leitlinie ist auch von der Hochschule beauftragten Dienstleistern, Gästen, die das Hochschulnetzwerk nutzen (wie z.B. Gastdozenten) und von allen externen Geschäfts- und Kooperationspartner, soweit diese entsprechend gebunden sind, verpflichtend einzuhalten.

3 Sicherheitsziele

Ziel der Informationssicherheit ist es, die Risiken, die für die Grundwerte der Informationssicherheit – Vertraulichkeit, Integrität und Verfügbarkeit – bestehen, auf ein akzeptables Maß zu reduzieren. Dies bedeutet, Informationen und Daten berechtigten Personen bei Bedarf in ausreichender Qualität zur Verfügung zu stellen und diese vor unberechtigter Manipulation und vor unberechtigtem Zugriff zu schützen. Die Informationssicherheit umfasst neben der Sicherheit der IT-Systeme und der darin

gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten Informationen. Die HNE Eberswalde verpflichtet sich, auch den Schutz von Informationen ihrer Geschäftspartner zu gewährleisten.

4 Sicherheitsstrategie und Maßnahmen

Zum Erreichen der Sicherheitsziele wird ein Informationssicherheitsmanagementsystem (ISMS), etabliert, das sich an der ISO 27001 orientiert.

Verantwortlich für Aufbau, Betrieb und Weiterentwicklung des ISMS ist der oder die Informationssicherheitsbeauftragte (ISB) der HNE Eberswalde. Dabei werden die zu schützenden Informationswerte analysiert und im Rahmen einer Risikoanalyse bewertet. Zur Bewertung von Risiken werden hochschulweit einheitliche Kriterien zur Risikoakzeptanz festgelegt. Diese Kriterien bilden den verbindlichen Rahmen für die Risikobeurteilung und dienen als Grundlage dafür, ob Risiken vermieden, reduziert, übertragen oder akzeptiert werden können. Es werden Verantwortlichkeiten und Vorgehensweisen festgelegt, um effektiv auf Sicherheitsvorfälle sowie Notfälle reagieren zu können. Schadensfälle mit hohen finanziellen oder immateriellen Auswirkungen sollen verhindert werden.

Zur Überprüfung der Wirksamkeit des Informationssicherheitsmanagementsystems führt die Hochschule in regelmäßigen Abständen interne Audits durch. Diese Audits bewerten die Einhaltung der definierten Sicherheitsvorgaben und unterstützen die kontinuierliche Verbesserung des ISMS. Die Planung und Durchführung der internen Audits erfolgt durch hierfür benannte Stellen in Zusammenarbeit mit dem Informationssicherheitsbeauftragten.

Das ISMS ist der Kern einer Sicherheitsstrategie, die dabei insbesondere folgende Maßnahmen umfasst, die sich jeweils an dem aktuellen Stand der Technik orientieren und mit einem vertretbaren Aufwand umzusetzen sind:

Sensibilisierung:

Die Hochschulangehörigen werden in die Lage versetzt, Gefahren für die Informationssicherheit zu erkennen und zu vermeiden. Der Stellenwert der Informationssicherheit muss allen bewusst werden

Risikoanalyse:

Im Rahmen einer ganzheitlichen Analyse der bestehenden Informationsverarbeitung, technisch wie konventionell, werden alle Elemente hinsichtlich ihrer Gefährdungen und der damit verbundenen Schadenshöhe bewertet.

Sicherheitsmaßnahmen:

Auf die Risikoanalyse aufbauend erfolgen die Auswahl und Umsetzung spezifischer Maßnahmen zur Behandlung dieser Risiken, insbesondere:

- Physische Sicherheit: Gebäude und Räumlichkeiten werden vor unberechtigtem Zutritt geschützt.
- Der Zugang zu IT-Systemen wird durch ein restriktives Berechtigungs- und Rollenkonzept in Verbindung mit Firewallsystemen und Sicherheitseinstellungen geschützt.

- Ein abgestuftes Datensicherungskonzept schützt vor dem Verlust wichtiger Daten
- Für sicherheitsrelevante Vorkommnissen werden Verantwortlichkeiten und Vorgehensweisen festgelegt, um schnell reagieren zu können und Schaden zu begrenzen
- Notfallpläne für Ausnahmefälle mit Meldeketten sollen festgelegt werden, um Schaden zu begrenzen und auch die Informationssicherheit in solchen Situationen zu gewährleisten
- Redundante IT-Systeme und Leitungswege sind notwendig, um die Verfügbarkeit zu erhöhen und Ausfallzeiten zu vermeiden
- Organisatorische Maßnahmen zur Erhöhung des Informationssicherheitsniveau
- Überwachung der Einhaltung der DSGVO und Compliance-Richtlinien der HNE Eberswalde

Werden Abweichungen von Sicherheitsanforderungen oder andere Nichtkonformitäten festgestellt, werden diese systematisch erfasst, bewertet und mit geeigneten Korrekturmaßnahmen behoben. Ziel ist es, Ursachen nachhaltig zu beseitigen und die Wirksamkeit der getroffenen Maßnahmen zu erhöhen. Die Umsetzung und Wirksamkeit der Korrekturmaßnahmen werden dokumentiert und überprüft.

Das Informationssicherheitsmanagementsystem umfasst eine strukturierte und nachvollziehbare Dokumentation aller relevanten Regelungen, Verfahren und Verantwortlichkeiten. Diese Dokumentation wird fortlaufend gepflegt und in aktualisierter Form bereitgestellt.

5 Verantwortung und Organisationsstruktur

Die Hochschulleitung der HNE Eberswalde trägt die Gesamtverantwortung für die Informationssicherheit. Sie erlässt verbindliche Regeln zur Informationssicherheit für die HNE Eberswalde und gibt sie den Mitarbeitenden und Studierenden bekannt. Sie stellt jederzeit eine Möglichkeit zur Kenntnisnahme der aktuellen Regeln sicher.

Um das definierte Sicherheitsniveau der HNE Eberswalde aufzubauen und aufrechtzuerhalten, stellt die Hochschulleitung alle erforderlichen Ressourcen zur Verfügung und fördert den kontinuierlichen Verbesserungsprozess der implementierten Sicherheitsmaßnahmen, Dokumente und festgelegten Informationssicherheitsprozesse.

Die Hochschulleitung setzt eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten (ISB) ein, welche*r für alle Belange der Informationssicherheit innerhalb der HNE Eberswalde zu ständig ist. Zudem bewertet diese Rolle das Informationssicherheitsmanagementsystem in regelmäßigen Abständen, um dessen Eignung, Angemessenheit und Wirksamkeit sicherzustellen. Ergebnisse dieser Managementbewertung fließen in die Weiterentwicklung der Sicherheitsstrategie und der erforderlichen Maßnahmen ein.

*Informationssicherheitsbeauftragte*r*

Die oder der ISB berät die Hochschulleitung in Fragen der Informationssicherheit und unterstützt bei der Umsetzung der Informationssicherheitsziele. Diese Rolle ist für alle operativen Belange und Fragen

zur Informationssicherheit zuständig, überprüft die Einhaltung der Sicherheitsrichtlinien und berichtet in dieser Funktion direkt an die Hochschulleitung.

Organisationseinheiten (Fachbereichsleitung, zentrale Bereich etc.)

Jede Organisationseinheit ist für die Sicherheit der eigenen Daten und deren Verarbeitung verantwortlich („Informationseigner“). Es liegt in der besonderen Verantwortung der Führungskräfte, die wirksame Umsetzung der Vorgaben zur Informationssicherheit ihrer Organisationseinheit zu überwachen und sicherzustellen.

*Datenschutzbeauftragte*r*

Der oder die von der Hochschulleitung ernannte Datenschutzbeauftragte (DSB) ist für alle operativen Belange und Fragen des Datenschutzes der Hochschule zuständig. Er unterstützte die ISB Rolle in ihrer Funktion und wirkt beratend am Informationssicherheitsmanagement in Belangen des Datenschutzes mit.

Hochschulangehörige:

Der Schutz aller Informationen, die im Rahmen der Geschäftsprozesse verarbeitet werden, ist grundsätzlich die Aufgabe aller Hochschulangehörigen und Mitglieder. Jeder Hochschulangehörige ist verpflichtet, die allgemeinen sowie die für den jeweiligen Arbeitsplatz geltenden Sicherheitsrichtlinien zu beachten und einzuhalten. Daher müssen alle Hochschulangehörige auch regelmäßig an den angebotenen Sicherheitsschulungen teilnehmen.

6 Inkrafttreten und Veröffentlichung

Diese Informationssicherheitsleitlinie tritt am Tag nach ihrer Veröffentlichung in Kraft. Sie wird allen Hochschulangehörigen bekannt gemacht.

Der Präsident

Unterzeichnet am 13. Mai 2026

Be advised! This text is a legally non-binding translation of the Information Security Policy (Leitlinie Informationssicherheit). When in doubt, please refer to the German text.

Information Security Policy

1 Importance of Information Processing

Information processing and information and communication technology in particular are of central importance for higher education institutions and research organizations in fulfilling their mission. It is embedded in all university processes. IT applications now form the basis for most processes. The range of IT applications includes computer-based information processing for research, teaching, and administration, as well as communication with external partners and clients.
The importance of information technology varies across research, teaching, and administration. Accordingly, disruptions or failures have impacts of differing severity.

The University Executive Board recognizes that the risks and expected impacts associated with information processing are changing and may come to pose an existential threat to the university.
With this policy, the University Executive Board underscores the importance of information security for the university and confirms that it assumes overall responsibility for the information security process.
The Information Security Policy is part of a tiered body of regulations and forms the basis for developing further subject-specific guidelines, information security concepts, and rules and directives on information security. In doing so, compliance with all statutory and contractual requirements relating to information security and data protection must also be ensured.

2 Scope

This policy is binding on all members and affiliates of the university, as well as on all organizational units of the university; it covers all business processes in teaching, research, and administration.
All members and affiliates of the university are obliged to cooperate responsibly in implementing the Information Security Policy.

The policy must also be complied with by service providers commissioned by the university, guests who use the university network (such as visiting lecturers), and all external business and cooperation partners, insofar as they are bound accordingly.

3 Security Objectives

The objective of information security is to reduce to an acceptable level the risks to the fundamental values of information security: confidentiality, integrity, and availability. This means making information and data available to authorized persons in sufficient quality when needed, while protecting them against unauthorized manipulation and unauthorized access. In addition to the security of IT systems and the data stored in them, information security also covers the security of information that is not processed electronically. HNEE is committed to ensuring the protection of its business partners' information as well.

4 Security Strategy and Measures

To achieve the security objectives, an Information Security Management System (ISMS) is established, based on ISO 27001.

Responsibility for establishing, operating, and further developing the ISMS lies with the Information Security Officer (ISB) of HNEE. The information assets to be protected are analyzed and assessed as part of a risk analysis. University-wide, uniform criteria for risk acceptance are defined for evaluating risks. These criteria form the binding framework for risk assessment and serve as the basis for deciding whether risks can be avoided, reduced, transferred, or accepted. Responsibilities and procedures are defined to enable an effective response to security incidents and emergencies. Damage events with significant financial or non-material impact are to be prevented.

To review the effectiveness of the Information Security Management System, the university conducts internal audits at regular intervals. These audits assess compliance with the defined security requirements and support the continual improvement of the ISMS. The internal audits are planned and carried out by designated bodies in cooperation with the Information Security Officer.
The ISMS is the core of a security strategy that in particular comprises the following measures, each of which is based on the current state of the art and implemented with a reasonable level of effort:

Awareness:

Members and affiliates of the university are enabled to recognize and avoid threats to information security. Everyone must become aware of the importance of information security.

Risk analysis:

As part of a holistic analysis of existing information processing, both technical and conventional, all elements are assessed with regard to their threats and the associated extent of potential damage.

Security measures:

Building on the risk analysis, specific measures to address these risks are selected and implemented, in particular:

- Physical security: buildings and premises are protected against unauthorized access.
- Access to IT systems is protected by a restrictive authorization and role concept in conjunction with firewall systems and security settings.
- A tiered data backup concept protects against the loss of important data.
- Responsibilities and procedures are defined for security-relevant incidents, to enable a rapid response and limit damage.
- Emergency plans with reporting/escalation chains are to be defined for exceptional situations, in order to limit damage and ensure information security even in such situations.
- Redundant IT systems and network paths are necessary to increase availability and avoid downtime.
- Organizational measures to raise the level of information security.
- Monitoring of compliance with the GDPR and HNEE's compliance policies.

If deviations from security requirements or other nonconformities are identified, they are systematically recorded, assessed, and remedied through appropriate corrective actions. The aim is to eliminate root causes sustainably and to increase the effectiveness of the measures taken. The implementation and effectiveness of corrective actions are documented and reviewed.

The Information Security Management System includes structured and traceable documentation of all relevant rules, procedures, and responsibilities. This documentation is maintained on an ongoing basis and made available in an up-to-date form.

5 Responsibility and Organizational Structure

The University Executive Board of HNEE bears overall responsibility for information security. It issues binding rules on information security for HNEE and communicates them to staff and students. It ensures at all times that the current rules can be accessed and reviewed.

To establish and maintain HNEE's defined level of security, the University Executive Board provides all necessary resources and promotes the continual improvement process of the implemented security measures, documents, and defined information security processes.

The University Executive Board appoints an Information Security Officer (ISB), who is responsible for all matters of information security within HNEE. This role also evaluates the Information Security Management System at regular intervals to ensure its suitability, adequacy, and effectiveness. The results of this management review feed into the further development of the security strategy and the required measures.

Information Security Officer (ISB)

The ISB advises the University Executive Board on matters of information security and supports the implementation of the information security objectives. This role is responsible for all operational matters and questions relating to information security, reviews compliance with the security policies, and reports directly to the University Executive Board in this capacity.

Organizational units (faculty management, central units, etc.)

Each organizational unit is responsible for the security of its own data and its processing ("asset owner"). It is the particular responsibility of managers to monitor and ensure the effective implementation of the information security requirements within their organizational unit.

Data Protection Officer (DPO)

The Data Protection Officer (DPO) appointed by the University Executive Board is responsible for all operational matters and questions relating to data protection at the university. The DPO supports the ISB in this function and provides advisory input to information security management on data protection matters.

Members and affiliates of the university:

Protecting all information processed as part of business processes is, in principle, the responsibility of all members and affiliates of the university. Every member of the university is obliged to observe and comply with the general security policies as well as those applicable to their specific workplace. All members and affiliates of the university must therefore also take part in the security training offered regularly.

6 Entry into Force and Publication

This Information Security Policy enters into force on the day after its publication. It is communicated to all members and affiliates of the university.

The President

Signed the 13th May 2026