Comprehensive IT Policy and Security Governance Framework

German University of Digital Science

IT Department

Prepared by: Yahya Narvil

Version 1.0 June 2025

Document Classification: Official - For Distribution
Review Date: June 2026
Distribution: University Stakeholders
Author: Yahya Narvil - IT Department

Contents

1 Executive Summary

German University of Digital Science requires a sophisticated IT governance approach that accommodates the unique needs of three distinct stakeholder groups while maintaining the flexibility essential for academic environments. This framework leverages the ITIL v4 Service Value System to create a balanced governance structure that supports educational excellence while ensuring robust security and compliance.

The framework addresses the complex requirements of modern university IT environments, including BYOD policies, research data protection, student privacy requirements, and compliance with German and European Union regulations. By implementing this comprehensive governance structure, German University of Digital Science will establish clear accountability, minimize security risks, and optimize IT service delivery across all stakeholder groups.

2 ITIL v4 Foundation and Service Value System Integration

2.1 Service Value System Components

The ITIL v4 Service Value System serves as the foundational framework for all IT governance activities at German University of Digital Science. The system encompasses five critical components that work together to enable value creation across all stakeholder groups.

2.1.1 Guiding Principles Implementation

- **Focus on Value:** All IT services prioritize educational outcomes and research support
- **Start Where You Are:** Leverage existing university infrastructure and processes
- **Progress Iteratively with Feedback:** Implement changes through controlled phases with stakeholder input
- **Collaborate and Promote Visibility:** Ensure transparent communication across all university levels
- **Think and Work Holistically:** Consider impact on students, staff, and administrators simultaneously
- **Keep It Simple and Practical:** Maintain usability while ensuring security compliance
- **Optimize and Automate:** Streamline processes while preserving academic flexibility

2.2 Four Dimensions of Service Management

2.2.1 Organizations and People

The governance structure recognizes the diverse needs of academic environments while maintaining clear accountability. Students require accessible self-service capabilities, staff need reliable

research and administrative tools, and IT administrators must maintain comprehensive system oversight.

2.2.2 Information and Technology

All technology decisions consider German data protection requirements under GDPR and BDSG while supporting academic freedom. The framework prioritizes data security without compromising research capabilities or educational accessibility.

2.2.3 Partners and Suppliers

Vendor relationships must comply with university procurement policies and European data protection standards. All external partnerships require risk assessment and compliance verification before implementation.

2.2.4 Value Streams and Processes

Service delivery processes accommodate the cyclical nature of academic calendars while maintaining consistent availability for critical systems. Emergency procedures account for academic deadlines and research continuity requirements.

3 Stakeholder-Specific Governance Framework

3.1 Students: Limited Privilege Access Model

3.1.1 Access Control and Authentication

Students receive time-limited accounts with access scoped to educational resources and approved research tools. Multi-factor authentication requirements balance security with usability, utilizing university-issued credentials combined with personal device verification.

3.1.2 BYOD Policy Implementation

The Bring Your Own Device policy accommodates diverse student technology preferences while maintaining security standards. Device registration requires security compliance verification including updated operating systems, active antivirus protection, and encrypted storage capabilities.

3.1.3 Privacy Protection and Academic Freedom

Student data protection follows both FERPA and GDPR requirements, ensuring educational record confidentiality while supporting legitimate academic research. Academic freedom protections allow students to access necessary research materials within ethical and legal boundaries.

3.1.4 Key ITIL Practices for Students

- **Service Desk:** 24/7 support for educational technology issues with multilingual capabilities
- **Service Request Management:** Self-service portal for common requests including software installations and access permissions
- **Availability Management:** Guaranteed system availability during critical academic periods including registration and examination windows
- **Service Catalogue Management:** Clear documentation of available educational technology services and access procedures

3.2 Staff: Business-Critical Access Framework

3.2.1 Enhanced Security Protocols

Staff members receive elevated access privileges commensurate with their academic and administrative responsibilities. Role-based access control ensures appropriate system permissions while maintaining audit trails for compliance verification.

3.2.2 Research Data Protection

Specialized protocols protect sensitive research data while facilitating collaborative academic work. Data classification systems ensure appropriate handling of confidential information including student records, research findings, and administrative documents.

3.2.3 Knowledge Management Systems

Comprehensive knowledge repositories support academic collaboration while maintaining version control and access logging. Integration with existing academic systems ensures seamless workflow for teaching and research activities.

3.2.4 Key ITIL Practices for Staff

- **Information Security Management:** Comprehensive security awareness training and policy enforcement
- **Service Level Management:** Defined performance standards for critical academic and research systems
- **Knowledge Management:** Centralized documentation and best practice sharing platforms
- **Change Control:** Structured approval processes for system modifications affecting academic operations

3.3 IT Administrators: Full System Access and Responsibility

3.3.1 Privileged Access Management

IT administrators operate under enhanced security protocols including continuous monitoring, regular access reviews, and mandatory security training. Administrative actions require dual authorization for critical system changes and comprehensive audit logging.

3.3.2 Infrastructure Security Controls

Implementation of defense-in-depth strategies protects university systems from evolving cyber threats. Regular vulnerability assessments and penetration testing ensure proactive security posture while maintaining system availability for academic operations.

3.3.3 Incident Response and Management

Rapid response capabilities address security incidents while minimizing impact on academic operations. Clear escalation procedures ensure appropriate notification of stakeholders while maintaining operational security.

3.3.4 Key ITIL Practices for IT Administrators

- **Information Security Management:** Leadership of university-wide security initiatives and policy development
- **Infrastructure and Platform Management:** Comprehensive system administration and capacity planning
- **Incident Management:** Rapid resolution of system issues with clear communication protocols

- **Problem Management:** Root cause analysis and preventive measures to reduce recurring issues
- **Continual Improvement:** Regular assessment and enhancement of IT services and security posture

4 Compliance and Regulatory Framework

4.1 Monitoring and Audit Mechanisms

4.1.1 Continuous Compliance Monitoring

Automated compliance monitoring systems track adherence to policies and regulations while generating regular reports for governance committees. Real-time dashboards provide visibility into key performance indicators and compliance metrics.

4.1.2 Regular Assessment Cycles

Quarterly compliance reviews assess policy effectiveness and identify areas for improvement. Annual risk assessments evaluate emerging threats and regulatory changes to ensure continued compliance.

4.1.3 Stakeholder Feedback Integration

Regular surveys and feedback sessions with students, staff, and administrators provide input for policy refinement and service improvement. Academic calendar considerations ensure feedback collection aligns with university operational cycles.

5 Risk Management and Enforcement Framework

5.1 Risk Assessment and Mitigation

5.1.1 Comprehensive Risk Management

The university employs a structured risk management approach that considers academic, operational, and regulatory risks. Risk registers document identified threats and mitigation strategies while providing clear ownership and accountability.

5.1.2 Academic-Specific Risk Considerations

Unique university risks including research data protection, student privacy, and academic freedom receive specialized attention in risk assessments. Mitigation strategies balance security requirements with academic operational needs.

5.2 Enforcement and Violation Management

5.2.1 Graduated Response Framework

Policy violations trigger proportionate responses based on severity and impact. Minor infractions result in training and remediation, while serious violations may require access suspension or disciplinary action.

5.2.2 Appeal and Review Processes

Clear appeal procedures ensure fair treatment of policy violations while maintaining institutional security. Academic freedom protections provide additional safeguards for legitimate research and educational activities.

6 Prohibition of Private Domain Login Data Sharing and Related Controls

6.1 Policy Statement

University-issued domain credentials (such as usernames and passwords) must not be shared with any third party, including external service providers, collaborators, or unauthorized university members. Use of university login credentials for non-university (private or external) platforms is strictly prohibited to prevent credential leakage and unauthorized access.

6.2 Account Usage Restrictions

Access to university systems and resources must only be performed using officially assigned university accounts. Personal or private domain accounts (e.g., private email or cloud accounts) may not be used to access or store university data, especially sensitive or confidential information. Integration or linking of private accounts with university systems (such as using personal email for password recovery or authentication) is not permitted unless explicitly authorized by IT governance.

6.3 Data Sharing Controls

All data sharing, whether internal or external, must comply with university data governance protocols and relevant legal frameworks such as GDPR and the EU Data Act. Data sharing with third parties is only allowed under a formal agreement that specifies the purpose, scope, and security measures for data access and handling. Sharing of data that includes login credentials, authentication tokens, or any information that could compromise access control is strictly forbidden.

6.4 Authentication and Audit Enforcement

Authentication policies must enforce that privileged accounts are only used on authorized, university-managed devices and never on personal or untrusted systems. Multi-factor authentication is mandatory for all domain accounts with elevated privileges. Regular audits will be conducted to detect and remediate any unauthorized sharing or use of domain login data.

6.5 Incident Reporting

Any suspected or confirmed incident of domain login data sharing or unauthorized access must be reported immediately to the IT security team for investigation and response. The university reserves the right to suspend or revoke access for accounts involved in policy violations pending investigation.

6.6 User Awareness

All users must complete annual security awareness training, including modules on the risks of credential sharing and the importance of protecting domain login data. Regular reminders and updates will be provided to reinforce best practices in credential management and data sharing.

7 Performance Metrics and Key Performance Indicators

7.1 Governance Effectiveness Indicators

7.1.1 Policy Compliance Metrics

Regular measurement of policy adherence across all stakeholder groups ensures effective governance implementation. Automated monitoring systems track compliance rates and identify

areas requiring additional attention or training.

7.1.2 Stakeholder Engagement Metrics

Active participation in governance processes demonstrates stakeholder buy-in and framework effectiveness. Regular surveys and feedback sessions provide quantitative and qualitative measures of engagement success.

8 Conclusion and Success Metrics

This comprehensive IT governance framework provides German University of Digital Science with a robust foundation for secure, efficient, and compliant technology operations. The integration of ITIL v4 principles ensures world-class service delivery while accommodating the unique requirements of academic environments.

Success measurement focuses on key performance indicators including service availability, incident resolution times, user satisfaction scores, and compliance metrics. Regular review and refinement processes ensure the framework evolves with changing university needs and regulatory requirements.

The framework's immediate implementability combined with its comprehensive coverage of stakeholder needs positions German University of Digital Science for sustained success in an increasingly digital academic environment. Continuous improvement processes embedded throughout the framework ensure long-term effectiveness and adaptability to emerging challenges and opportunities.

Document Control

Document Title	Comprehensive IT Policy and Security Governance Framework
Version	1.0
Date	June 2025
Author	Yahya Narvil - IT Department
Institution	German University of Digital Science
Next Review	June 2026
Distribution	University Stakeholders
Classification	Official - For Distribution

Contact Information:

- IT Department: itadmin@german-uds.de

A Appendix A: Official University Confirmation

The following document provides official confirmation and authorization from German University of Digital Science for this IT Governance Framework implementation. This confirmation validates the authority and institutional support for the comprehensive governance structure outlined in this framework.