

IT-Sicherheitsleitlinie

der

Stiftung Preußischer Kulturbesitz



**Stiftung
Preußischer Kulturbesitz**

Inhalt

1	Einleitung	3
2	Gegenstand und Geltungsbereich	3
3	Stellenwert der Informationsverarbeitung	4
3.1	Grundsätze der Sicherheitspolitik und Sicherheitskultur	4
3.2	Anforderungen durch die verarbeiteten Daten	5
3.3	Angemessenheit von Sicherheitsmaßnahmen.....	5
3.4	Beratung, Schulung und Sensibilisierung	5
3.5	Bereitstellung von ausreichenden Ressourcen für die Informationssicherheit	5
4	Sicherheitsmanagement / Verantwortlichkeiten	5
4.1	Organisationsstruktur zur Umsetzung des IT-Sicherheitsprozesses	6
4.2	Aufgaben und Verantwortung innerhalb der Organisationsstruktur	6
5	Sicherheitsmaßnahmen.....	8
6	Verbesserung der Informationssicherheit	9

1 Einleitung

Die Stiftung Preußischer Kulturbesitz (SPK) ist eine weltweit renommierte Kultureinrichtung und ein bedeutender Akteur in den Geistes- und Sozialwissenschaften. Zu ihr gehören Museen, Bibliotheken, Archive und Forschungsinstitute. Ihre Sammlungen haben universalen Charakter. Sie dokumentieren die kulturelle Entwicklung der Menschheit von den Anfängen bis in die Gegenwart, in Europa wie in anderen Kontinenten. Sie sind in Brandenburg und Preußen entstanden und enzyklopädisch gewachsen. Heute wirkt die Stiftung an der Neugestaltung der historischen Mitte Berlins wesentlich mit.

Unter dem Dach der Stiftung sind fünf Einrichtungen vereint: die Staatlichen Museen zu Berlin, die Staatsbibliothek zu Berlin, das Geheime Staatsarchiv Preußischer Kulturbesitz, das Ibero-Amerikanische Institut und das Staatliche Institut für Musikforschung. Alle Sparten der kulturellen Überlieferung sind damit in der Stiftung vertreten.

Mit rund 2000 Mitarbeiterinnen und Mitarbeitern ist die Stiftung deutschlandweit die größte Arbeitgeberin im Kulturbereich. Sie ist eine bundesunmittelbare Stiftung und von der föderalen Struktur Deutschlands geprägt. Der Bund und alle sechzehn Bundesländer tragen und finanzieren sie gemeinschaftlich. Sitz der Stiftung Preußischer Kulturbesitz und aller ihrer Einrichtungen ist Berlin.

Den Anforderungen an die zukünftige Bewahrung des kulturellen Erbes kann die SPK nur gerecht werden, wenn bei der elektronischen Verarbeitung die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen garantiert werden kann. Dabei sind auch alle informationssicherheitsrelevanten gesetzlichen Vorschriften zu berücksichtigen, insbesondere die des Datenschutzes.

Die SPK muss den Informationssicherheitsprozess konkretisieren, steuern und kontrollieren. Dazu gehören strategische Leitaussagen zur Informationssicherheit, konzeptionelle Vorgaben und auch organisatorische Rahmenbedingungen, um Informationssicherheit innerhalb aller Geschäftsprozesse erreichen zu können.

Die IT-Sicherheitsleitlinie (ITSL) gibt als Generalfestlegung für die SPK allgemeine strategische Ziele, wie die Gewährleistung des sicheren und ordnungsmäßigen IT-Einsatzes bei der Aufgabenerfüllung sowie die Beachtung und Durchsetzung des Datenschutzes vor.

Die vorliegende Leitlinie zur Informationssicherheit beschreibt den Rahmen für die Sicherheit der Informationsverarbeitung in den Einrichtungen der SPK. Sie legt die Ziele und Grundsätze für die Informationssicherheit fest. Alle Beschäftigten der SPK sind angehalten, in diesem Sinne verantwortungsbewusst zu handeln.

2 Gegenstand und Geltungsbereich

Die IT-Sicherheitsleitlinie (ITSL) definiert den Rahmen des Sicherheitsstandards der SPK und dient damit als Grundlage für ein SPK-weites Sicherheitskonzept sowie weiterführender Konzepte. In ihrer Gesamtheit bilden diese Dokumente das SPK-Regelwerk zur Informationssicherheit.

Die ITSL trifft generelle, allgemeingültige Aussagen zum angestrebten IT-Sicherheitsniveau und zur IT-Sicherheitsstrategie für alle Beschäftigten, Organisationseinheiten und Einrichtungen der gesamten SPK.

Die ITSL ist auch von externen Beratern, für Dienstleistern sowie für allen Partnern und Lieferanten, die mit der SPK in informationsverarbeitenden Beziehungen stehen, zu beachten. Hierfür sind gegebenenfalls vertragliche Vereinbarungen zu treffen, die der ITSL gerecht werden.

3 Stellenwert der Informationsverarbeitung

Dem herausragenden Renommee der SPK als Wissenschafts- und Forschungsinstitution und insbesondere dem Anspruch, eine moderne, dynamische und zukunftsorientierte Einrichtung zu sein, gilt es gerecht zu werden. Die Bewahrung, Aufarbeitung und Bereitstellung der in verschiedenen Ausprägungen vorhandenen kulturellen Überlieferungen (Objekt-, Bild-, Text- und Tonquellen) in digitaler Form sind dabei für die Zukunft von besonderer Bedeutung. Die Erkenntnisse aus der wissenschaftlichen Erschließung und Erforschung der Wissensarchive macht die SPK weltweit verfügbar und leistet damit einen wichtigen Beitrag zur globalen Wissens- und Informationsgesellschaft. Der Öffentlichkeit sowie anderen kulturellen und wissenschaftlichen Einrichtungen soll ein komfortabler Zugang zu den historischen und modernen Quellen oder elektronischen Ressourcen gewährt werden.

Die Informationstechnik (IT) bildet dabei die Basis für die Kern- und Geschäftsprozesse. Sie ermöglicht eine Optimierung der Abläufe, unterstützt die Beschäftigten in ihrer täglichen Aufgabenerfüllung und bietet der SPK zusätzlich die Möglichkeit, vertrauensvoll und schnell mit externen Partnern zu kommunizieren. Durch eine nicht zuverlässig verfügbare, kompromittierbare IT-Infrastruktur werden ggf. die Schutzziele „Vertraulichkeit“, „Verfügbarkeit“, und „Integrität“ verletzt. Es besteht die Gefahr von materiellen und/oder ideellen Schäden. Damit kann das Image der SPK nachhaltig geschädigt werden bzw. können mühevoll oder langjährige zusammengetragene Informationen oder Forschungsergebnisse verloren gehen.

3.1 Grundsätze der Sicherheitspolitik und Sicherheitskultur

- Gesamtverantwortlich für die Informationssicherheit der SPK ist der Präsident. Grundsätzliche Festlegungen zur Informationssicherheit werden bei der SPK durch den Präsidenten getroffen.
- Die Beschäftigten sollen bei der Erstellung, Nutzung und Verwaltung von Daten und Informationen die ITSL und andere stiftungsinterne Regelungen mit Bezug zur Informationssicherheit beachten und alle darüber hinaus geltenden (gesetzlichen) Vorschriften einhalten. Erkannte Schwachstellen müssen umgehend an den IT-Sicherheitsbeauftragten der jeweiligen Einrichtung gemeldet werden. Innerhalb der SPK wird in einrichtungsübergreifenden Gremien über Sicherheitslücken und über Sicherheitsvorfälle informiert.

3.2 Anforderungen durch die verarbeiteten Daten

Bei der SPK werden auf den IT-Systemen und über die Kommunikationswege Daten verarbeitet, die jeweils unterschiedliche Schutzbedarfe zur Be- und Verarbeitung beinhalten.

Neben der Vertraulichkeit insbesondere für personenbezogene Daten bestehen für eine Vielzahl der Datensammlungen hohe Anforderungen an die Integrität und Verfügbarkeit. Eine unberechtigte Änderung oder Zerstörung der Daten kann zu bedeutenden finanziellen Verlusten bzw. zu einem beträchtlichen Imageverlust der SPK führen. Diesen Ansprüchen muss die SPK gerecht werden.

3.3 Angemessenheit von Sicherheitsmaßnahmen

Aufwand und Ziele der Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zueinander stehen. Neben der Beachtung gesetzlich vorgeschriebener Sicherheitsanforderungen müssen die getroffenen Sicherheitsmaßnahmen zugleich auch immer nachprüfbar im Verhältnis zu Schutzzweck und Schutzbedarf stehen. Die Angemessenheit von Maßnahmen ist im Rahmen der geltenden haushaltsrechtlichen Vorschriften zu dokumentieren. Es gilt der Grundsatz: „Risiko erkennen, Risiko bewerten, Risiko behandeln!“. Bei der Auswahl und Umsetzung von Sicherheitsmaßnahmen ist darauf zu achten, dass der Ablauf von Geschäftsprozessen bzw. der Zugriff auf Datenbestände durch angemessene Sicherheitsmaßnahmen begleitet wird.

3.4 Beratung, Schulung und Sensibilisierung

Die Sensibilisierung für Informationssicherheit, die fachliche Beratung und Schulungen der Mitarbeiterinnen und Mitarbeiter sind wichtige Voraussetzungen zur Etablierung einer angemessenen Informationssicherheit.

Die SPK schafft durch einschlägige, regelmäßige Schulungsangebote die entsprechenden Rahmenbedingungen. Hierbei ist insbesondere darauf zu achten, dass Fehlverhalten durch Unkenntnis oder Missachtung der Sicherheitsbestimmungen oder aus fehlender Übung im Umgang mit bereits etablierten Schutzmaßnahmen vorgebeugt werden kann.

Die fachlichen Qualifikationen der IT-Sicherheitsbeauftragten (IT-Sibe) bei der SPK werden durch Fortbildungsangebote im erforderlichen Umfang gefördert.

3.5 Bereitstellung von ausreichenden Ressourcen für die Informationssicherheit

Um ein angemessenes Maß an Informationssicherheit zu erreichen und aufrecht zu erhalten, sind durch die SPK personelle, zeitliche und finanzielle Ressourcen bereitzustellen.

4 Sicherheitsmanagement

Durch das Zusammenwirken der IT-Sicherheitsbeauftragten der Einrichtungen soll die Erreichung der Informationssicherheitsziele gewährleistet werden. Die nachfolgend beschriebene

**Sicherheitsorganisation
der Stiftung Preußischer Kulturbesitz**

Präsident

- Hauptpersonalrat
- Datenschutzbeauftragte
- Fortbildungsbeauftragte

AG-IT Sibe (Arbeitsgruppe der IT-Sicherheitsbeauftragten)

- IT-Sibe der (HV)
- IT-Sibe der Einrichtung (SMB)
- IT-Sibe der Einrichtung (SBB)
- IT-Sibe der Einrichtung (GStA)
- IT-Sibe der Einrichtung (SIM)
- IT-Sibe der Einrichtung (IAI)

Hauptverwaltung (HV)

- Staatliche Museen zu Berlin (SMB)
- Staatsbibliothek zu Berlin (SBB)
- Geheimes Staatsarchiv (GStA)
- Staatliches Institut für Musikforschung (SIM)
- Ibero-Amerikanisches Institut (IAI)

Arbeitsgruppe Rechenzentrum (AG-RZ)

Vertreter (HV)	Vertreter (SMB)	Vertreter (SBB)
Vertreter (GStA)	Vertreter (SIM)	Vertreter (IAI)
Hauptpersonalrat	Datenschutzbeauftragte	

Koordinierung des strategischen IT-Service

Arbeitsgruppe IT (AG-IT)

Vertreter (HV)	Vertreter (SMB)	Vertreter (SBB)
Vertreter (GStA)	Vertreter (SIM)	Vertreter (IAI)
Personalvertretung (SMB)	Personalvertretung (SBB)	Hauptpersonalrat

Koordinierung der operativen IT-Systeme
Koordinierung von einrichtungsübergreifenden Themen der Informationstechnik
Konzeptionierung und Realisierung der stiftungsweiten Infrastruktur

Festlegungen als Basis für Arbeit

Das angestrebte Sicherheitsniveau der SPK kann nur erreicht werden, wenn in der gesamten Stiftung die erforderlichen Maßnahmen umgesetzt werden. Hierzu müssen Rollen innerhalb der SPK festgelegt und Aufgaben und Verantwortlichkeiten zugeordnet werden. Diese Rollen müssen anschließend qualifizierten Mitarbeitern übertragen werden. Nur so kann gewährleistet werden, dass alle wichtigen Aspekte berücksichtigt und sämtliche anfallenden Aufgaben effizient und effektiv erledigt werden.

4.2 Aufgaben und Verantwortung innerhalb der Organisationsstruktur

6

Präsident

Der Präsident der SPK ist für die Erstellung, Aktualisierung und Umsetzung der Leitlinie zur Informationssicherheit verantwortlich. Er kann diese Aufgabe delegieren.

Einrichtungsleitungen

Die Einrichtungsleitungen verantworten die Umsetzung der IT-Sicherheitsleitlinie nebst den erforderlichen, konkreten Maßnahmen in ihrem Zuständigkeitsbereich. Sie unterstützen die IT-SiBe u.a. durch die Zurverfügungstellung von angemessenen zeitlichen und finanziellen Ressourcen zur Weiterbildung.

IT-Sicherheitsbeauftragte

In jeder Einrichtung wird die Rolle eines IT-Sicherheitsbeauftragten wahrgenommen. Er soll über fundierte IT-Kenntnisse verfügen, muss aber nicht der IT-Abteilung seiner Einrichtung angehören. Der IT-Sicherheitsbeauftragte unterstützt und berät sowohl Fachabteilungen als auch die IT-Abteilungen und die jeweilige Einrichtungsleitung in Fragen der IT-Sicherheit. Hierzu gehören insbesondere die Implementierung bzw. Veranlassung zentraler und Kontrolle dezentraler Sicherheitsmaßnahmen in seiner Einrichtung. Darüber hinaus obliegen ihm die Führung der Dokumentation zur IT-Sicherheit sowie die Mitarbeit an der Fortschreibung des IT-Sicherheitskonzeptes und die Abstimmung mit dem Sibe der Hauptverwaltung im Rahmen der unten formulierten Aufgaben.

Der IT-Sicherheitsbeauftragte der Einrichtung gehört der AG IT-Sibe an. Seine Aufgaben konzentrieren sich in diesem Zusammenhang auf die Erbringung von Unterstützungsleistungen bei der Umsetzung von Vorgaben des IT-Sicherheitsmanagements für die jeweilige Einrichtung. Der IT-Sicherheitsbeauftragte ist außerdem bei allen größeren Projekten, die deutliche Auswirkungen auf die Informationsverarbeitung haben, so wie bei der Einführung neuer Anwendungen und IT-Systeme zu beteiligen, um die Beachtung von Sicherheitsaspekten in den verschiedenen Projektphasen zu gewährleisten.

Der IT-Sicherheitsbeauftragte der Einrichtungen ist für alle Sicherheitsbelange der IT-gestützten Geschäftsprozesse, Anwendungen und IT-Systeme in seiner Einrichtung zuständig.

Zu den wesentlichen Aufgaben der IT-Sicherheitsbeauftragten gehören:¹

- auf die Umsetzung der Sicherheitsmaßnahmen gemäß IT-Sicherheitsleitlinie oder anderer spezifischer Sicherheitsleitlinien hinzuwirken,
- der Leitung und der AG-IT Sibe über den Status quo der Informationssicherheit zu berichten,
- als Ansprechpartner der Beschäftigten vor Ort zu dienen,
- Informationen über Schulungs- und Sensibilisierungsbedarf von Beschäftigten ermitteln,
- eventuell auftretende sicherheitsrelevante Zwischenfälle den Gremien AG IT-Sibe und AG-IT zu berichten.

Darüber hinaus obliegen dem IT-Sibe der HV folgende Aufgaben:

¹ vgl. BSI-Standard 100-2

- die Erstellung des Sicherheitskonzepts, des Notfallvorsorgekonzepts und anderer Teilkonzepte zu koordinieren, seine Inhalte gesamtheitlich zu verantworten und für die regelmäßige Aktualisierung zu sorgen.

Arbeitsgruppe der IT-Sicherheitsbeauftragten (AG IT-Sibe)

Der AG IT-Sibe gehören die IT-Sicherheitsbeauftragten der Einrichtungen an. Sie überprüft in regelmäßigen Abständen,

- ob neue Risiken zu bewerten sind ,
- ob die ITSL noch aktuell und zukunftssicher ist und
- überwacht den Umsetzungsstand der der Sicherheitsmaßnahmen.

Die AG IT-Sibe wird gemeinsam durch SMB und SBB als größte Einrichtungen der SPK geleitet, die operative Leitung wechselt periodisch einmal im Jahr.

Die Arbeitsgruppen Rechenzentrum (AG-RZ) und Informationstechnik (AG-IT) werden nach Bedarf in Fragen der IT-Sicherheit beraten. Zur Dokumentation der Sicherheitsarchitektur der SPK und zur Unterstützung der Erstellung des IT-Sicherheitskonzeptes wird eine vom BSI empfohlene Applikation eingesetzt.

Datenschutzbeauftragte der SPK

Die Datenschutzbeauftragte hat unter anderem die IT-Sicherheitsbeauftragten zu Fragen der Verarbeitung von personenbezogenen Daten zu beraten.

Beschäftigte der SPK

Angemessene Informationssicherheit kann nur realisiert werden, wenn alle Beschäftigten der SPK achtsam, verantwortungs- und sicherheitsbewusst handeln, um sowohl materiellen als auch ideellen Schaden, respektive Imageverlust, von der SPK abzuwenden.

5 Sicherheitsmaßnahmen

Die SPK nutzt den IT-Grundschutz als Sicherheitsstandard von IT-Systemen, den das Bundesamt für Sicherheit in der Informationstechnik (BSI) geschaffen hat. Mit den dort beschriebenen Maßnahmen soll das Risiko für IT-Infrastruktur, IT-Anwendungen und Informationen so gering wie möglich gehalten werden, damit weitgehend sichergestellt werden kann, dass eventuelle Ereignisse in ihrer schädigenden Auswirkung begrenzt werden können.

Die Sicherheitsmaßnahmen orientieren sich an den jeweiligen im IT-Sicherheitskonzept definierten Schutzbedarfen. Es soll sichergestellt werden, dass Schutzbedarfe mit angemessenem Aufwand gedeckt werden können. Beispielhaft werden Gebäude und Räumlichkeiten durch ausreichende Zutrittskontrollen geschützt. Der Zugang zu IT-Systemen wird durch angemessene Zugangskontrollen und der Zugriff auf die Daten durch ein restriktives Berechtigungskonzept geschützt.

Computer-Viren-Schutzprogramme werden auf allen relevanten IT-Systemen eingesetzt. Eine geeignete Firewall sichert alle Internetzugänge. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz gewährleisten und Manipulationen verhindern. Des Weiteren unterstützen die IT-Benutzer durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten die zuständigen Stellen.

Verlust oder unbeabsichtigte Veränderungen von Daten können nie vollkommen ausgeschlossen werden. Daher wird durch eine umfassende Datensicherung gewährleistet, dass der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen oder offensichtlich fehlerhaft sind.

Um größere Schäden in Folge von Notfällen zu begrenzen bzw. diesen vorzubeugen, ist auf Sicherheitsvorfälle umgehend und konsequent zu reagieren. Maßnahmen für den Notfall werden in einem Notfallvorsorgekonzept zusammengestellt. Ziel der SPK ist es, auch bei einem Systemausfall kritische Geschäftsprozesse aufrecht zu erhalten und die Verfügbarkeit der ausgefallenen Systeme innerhalb einer definierten Zeitspanne wiederherzustellen.

Sofern IT-Dienstleistungen an externe Stellen ausgelagert werden, werden von der SPK konkrete Sicherheitsanforderungen in den jeweiligen Verträgen vereinbart.

6 Verbesserung der Informationssicherheit

Das IT-Sicherheitskonzept, die sonstigen Sicherheitsdokumente (wie z.B. Datensicherungs-, Zugriffs- und Notfallvorsorgekonzepte sowie die Sicherheitsorganisation werden regelmäßig auf ihre Aktualität und Wirksamkeit geprüft. Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der IT-Sicherheitstechnik zu halten. Veränderungen in den Geschäftsprozessen und die Weiterentwicklung der Technologien finden Berücksichtigung.

Die IT-Sicherheitsleitlinie wird im Intranet der SPK stets mit dem aktuellen Stand veröffentlicht und steht somit allen Mitarbeiterinnen und Mitarbeitern zur Verfügung.

Berlin, den 17.8.2016

gez. Prof. Dr. Hermann Parzinger
Präsident der Stiftung Preußischer Kulturbesitz