# IT-Sicherheitsrichtlinie der Max-Planck-Gesellschaft

Am 21.06.2017 vom Verwaltungsrat beschlossen

## Inhalt



## Präambel

Diese IT-Sicherheitsrichtlinie beruht auf der IT-Sicherheitsleitlinie der Max-Planck-Gesellschaft vom 21.06.2017 und konkretisiert die IT-Sicherheitsvorgaben für die Einrichtungen der Gesellschaft (Institute, Forschungsstellen, Generalverwaltung und zentrale Einrichtungen) und deren Mitarbeiterinnen und Mitarbeiter sowie Nutzerinnen und Nutzer ihrer IT-Infrastruktur.

Sie beschreibt die ständigen IT-Sicherheitsstrukturen der Max-Planck-Gesellschaft, deren Funktion und Zusammenwirken sowie die notwendigen Prozesse, um ein funktionsfähiges Managementsystem zur Steuerung der Informationssicherheit in der Max-Planck-Gesellschaft etablieren, betreiben und weiterentwickeln zu können.

Sie strebt an, hinreichend abstrakt zu sein, um unabhängig von konkreten Lösungen Vorgaben zu machen, aber spezifisch genug, um den Weg zur konkreten Umsetzung zu weisen. Angesichts der schnellen Entwicklungen in der Informationstechnologie muss sie flexibel genug auf neue Herausforderungen anwendbar und insbesondere offen für neue IT-Sicherheitskonzepte sein. Dabei definiert sie dennoch eine Reihe von Mindestanforderungen, die sicherstellen, dass das Handeln einer einzelnen Einrichtung keine negativen Auswirkungen auf andere Einrichtungen der Max-Planck-Gesellschaft oder die Max-Planck-Gesellschaft als Ganzes hat. Die Mindestanforderungen sollen auch die Einhaltung von Gesetzen, Verordnungen und Compliance-Vorgaben gewährleisten.

Sie orientiert sich an den Interessen der Max-Planck-Gesellschaft, ihrer Einrichtungen sowie ihrer Mitarbeiterinnen und Mitarbeitern. Diese gehen den persönlichen Interessen einzelner Personen vor.

Sie fordert die enge Zusammenarbeit aller Beteiligten, um der Dezentralität der IT-Infrastruktur der Max-Planck-Gesellschaft gerecht werden zu können. Nur durch einen offenen Austausch über IT-Sicherheitsvorfälle ist eine realistische Einschätzung der Bedrohungslage und die Auswahl der richtigen Maßnahmen möglich. Ein offener und sensibler Umgang mit Fehlern ist eine Voraussetzung für diesen Austausch.

Die IT-Sicherheitsrichtlinie hat die Integrität, Vertraulichkeit und Verfügbarkeit von Daten, Anwendungen und technischer Infrastruktur als Schutzziele. Die Erforderlichkeit von Maßnahmen zur IT-Sicherheit misst sich an den Anforderungen der wissenschaftlichen Projekte und der Erfüllung dienstlicher Aufgaben. Diese Maßnahmen sollen die Freiheit der Nutzerinnen und Nutzer im Allgemeinen, vor allem aber der Wissenschaftlerinnen und Wissenschaftler, nur im erforderlichen Umfang einschränken.

Die in der IT-Sicherheitsrichtlinie beschriebenen Prozesse müssen innerhalb einer angemessenen Frist umgesetzt werden.

# A. Organisatorische Strukturen

## A.1 Einrichtungsübergreifende Organisationsstrukturen

### 1. Der Verwaltungsrat der Max-Planck-Gesellschaft

Der Verwaltungsrat der Max-Planck-Gesellschaft trägt die Gesamtverantwortung für die IT-Sicherheit und sorgt für die nötige Priorität und Aufmerksamkeit für Fragen der IT-Sicherheit. Dazu beschließt er die IT-Sicherheitsleitlinie der Max-Planck-Gesellschaft und diese IT-Sicherheitsrichtlinie der Max-Planck-Gesellschaft.

### 2. Die IT-Sicherheitskommission der Max-Planck-Gesellschaft

Die gemäß der IT-Sicherheitsleitlinie einzurichtende IT-Sicherheitskommission besteht aus bis zu zehn Mitgliedern (einer Vizepräsidentin bzw. einem Vizepräsidenten (Vorsitz), mind. drei Direktorinnen und Direktoren, der bzw. dem IT-Sicherheitsbeauftragten der Max-Planck-Gesellschaft, der Sprecherin bzw. dem Sprecher des Kompetenznetzwerks IT-Sicherheit, je einer Vertreterin bzw. einem Vertreter der Mitarbeiterinnen und Mitarbeiter und des BAR sowie weiteren Personen). Die bzw. der Vorsitzende bestimmt aus dem Kreis der Direktorinnen und Direktoren unter den Kommissionsmitgliedern eine Stellvertreterin bzw. einen Stellvertreter. Dieser Person obliegt die operative fachkundige Leitung und Organisation des Gremiums soweit die bzw. der Vorsitzende diese nicht an sich zieht.

Sie legt dem Verwaltungsrat der Max-Planck-Gesellschaft bei Bedarf Vorschläge zur Anpassung der IT-Sicherheitsleitlinie und der IT-Sicherheitsrichtlinie vor. Beide Dokumente sollen mindestens alle fünf Jahre hinsichtlich ihres Aktualisierungsbedarfs durchgesehen werden und dem Verwaltungsrat zur erneuten Beschlussfassung vorgelegt werden.

Angesichts der Änderungsgeschwindigkeit in Anforderungen der IT-Sicherheit kann die IT-Sicherheitskommission anstelle des Verwaltungsrats bei dringendem Bedarf Anpassungen in Teil C dieser IT-Sicherheitsrichtlinie vornehmen. Der Verwaltungsrat ist nachlaufend zu informieren.

Die IT-Sicherheitskommission erlässt darüber hinaus in Ausfüllung der IT-Sicherheitsleitlinie und -richtlinie weitergehende Empfehlungen. Sie legt dem Verwaltungsrat jährlich einen Bericht zur Lage der IT-Sicherheit in der Max-Planck-Gesellschaft vor.

Bei einem besonders schwerwiegenden IT-Sicherheitsvorfall ruft die oder der Vorsitzende der IT-Sicherheitskommission einen Krisenstab ein und ergreift in Absprache mit der Präsidentin bzw. dem Präsidenten die erforderlichen Maßnahmen.

### 3. Die bzw. der IT-Sicherheitsbeauftragte der Max-Planck-Gesellschaft

Die bzw. der IT-Sicherheitsbeauftragte der Max-Planck-Gesellschaft wird vom Verwaltungsrat der Max-Planck-Gesellschaft bestellt und berichtet direkt an diesen. Sie bzw. er ist Mitglied der IT-Sicherheitskommission und unterstützt die Organe und die Einrichtungen der Gesellschaft bei der Erfüllung ihrer Aufgaben im Bereich der IT-Sicherheit. Ihr bzw. ihm werden die erforderlichen Ressourcen und Befugnisse zur Verfügung gestellt.

### 4. Das Kompetenznetzwerk IT-Sicherheit

Das Kompetenznetzwerk IT-Sicherheit wird aus den Spezialistinnen und Spezialisten für IT-Sicherheit in den Einrichtungen der Max-Planck-Gesellschaft und der bzw. dem IT-Sicherheitsbeauftragten der Max-Planck-Gesellschaft gebildet, die auf dem Gebiet der IT-Sicherheit zusammenarbeiten. Es erarbeitet für die IT-Sicherheitskommission detaillierte Vorschläge und steht den Einrichtungen und insbesondere deren IT-Gruppen als Ansprechpartner zur Verfügung. Es ist sowohl im Auftrag als auch selbstständig und proaktiv tätig und erarbeitet gegebenenfalls entsprechende Vorschläge. Insbesondere bereitet das Kompetenznetzwerk IT-Sicherheit Maßnahmen für den ernsten IT-Sicherheitsvorfall vor und unterstützt die kurzfristige Wiederherstellung der operativen Handlungsfähigkeit der Max-Planck-Gesellschaft.

Es wählt eine Sprecherin bzw. einen Sprecher, die bzw. der Mitglied der IT-Sicherheitskommission wird. Das Kompetenznetzwerk gibt sich eine Geschäftsordnung. Ihm werden die erforderlichen Ressourcen zur Verfügung gestellt.

## A.2 Einrichtungen

### 1. Die Leitung jeder Einrichtung

Die Leitung jeder Einrichtung trägt die Verantwortung für die IT-Sicherheit in ihrer Einrichtung. Sie definiert auf Basis des Risikomanagements das für ihre Einrichtung spezifische IT-Sicherheitsniveau und schafft die erforderlichen Rahmenbedingungen, um der IT-Sicherheit in ihrem Zuständigkeitsbereich den erforderlichen Stellenwert zu geben. Sie stellt die notwendigen Ressourcen für das Erreichen der IT-Sicherheitsziele zur Verfügung.

### 2. Die IT-Sicherheitsbeauftragten der Einrichtungen

Jede Leitung einer Einrichtung muss eine bzw. einen IT-Sicherheitsbeauftragten bestimmen, an die bzw. den die Zuständigkeit für IT-Sicherheit und deren Weiterentwicklung delegiert werden kann. Die IT-Sicherheitskommission beschließt dazu ein Muster für ein wirksames Delegationsschreiben. Diese Rolle kann auch von der IT-Leitung ausgeführt werden. Bei mehreren Standorten oder großen Einrichtungen mit unterschiedlichen Anforderungen ist es möglicherweise sinnvoll, die Aufgaben auf mehrere kooperierende IT-Sicherheitsbeauftragte zu verteilen.

Die IT-Sicherheitsbeauftragten handeln in Abstimmung mit der Leitung und der IT-Gruppe. Sie erstellen das spezifische IT-Sicherheitskonzept der Einrichtung, das regelmäßig neuen Anforderungen entsprechend überarbeitet werden muss und erarbeiten diejenigen Maßnahmen, die zur Verbesserung und Aufrechterhaltung der IT-Sicherheit ergriffen werden müssen. Sie sind verantwortlich für die Pflege und Weiterentwicklung der Dokumente der Einrichtung zur IT-Sicherheit.

### 3. Die IT-Gruppen und Verwaltungen der Einrichtungen

Die IT-Gruppen und Verwaltungen setzen die notwendigen technischen und organisatorischen IT-Sicherheitsmaßnahmen des IT-Sicherheitskonzeptes um. Dabei wählen sie die für die Einrichtung am besten passenden Lösungen.

### 4. Die zentralen Einrichtungen der Max-Planck-Gesellschaft

Die Generalverwaltung ergreift geeignete IT-Sicherheitsmaßnahmen für die von ihr betriebene Verwaltungs-IT und unterstützt die Einrichtungen der Max-Planck-Gesellschaft bei ihren IT-Sicherheitsanstrengungen.

Die zentralen IT-Einrichtungen der Max-Planck-Gesellschaft bieten institutsübergreifende Dienste mit angemessenem IT-Sicherheitsniveau an. Sie beteiligen sich aktiv am Kompetenznetzwerk IT-Sicherheit und unterstützen und ergänzen damit seine Arbeit, z.B. mit Diensten, Software-Werkzeugen, Schulungen und Schulungsmaterial.

### 5. Vorgesetzte und Verantwortliche

Die Verantwortung für Personal, Projekte, Geräte und Daten ist auch mit der Verantwortung für die damit zusammenhängende IT-Sicherheit verbunden. Diese Verantwortung umfasst auch die Einleitung und Umsetzung der notwendigen IT-Sicherheitsmaßnahmen sowie die Kontrolle ihrer Einhaltung durch die im Verantwortungsbereich tätigen Nutzerinnen und Nutzer der IT-Infrastruktur. Sie arbeiten mit der bzw. dem IT-Sicherheitsbeauftragten der Einrichtung bei der Festlegung des IT-Sicherheitsniveaus in ihrem Bereich zusammen.

### 6. Die Nutzerinnen und Nutzer

Die Regelungen im Bereich IT-Sicherheit sind für alle Nutzerinnen und Nutzer verbindlich. Diese sind verpflichtet, bei der Erfüllung der Aufgabe „IT-Sicherheit" kooperativ und verantwortungsbewusst mitzuwirken.

Alle Nutzerinnen und Nutzer der Informations- und Kommunikationstechnik übernehmen Verantwortung für die ordnungsgemäße Nutzung der von ihnen eingesetzten Dienste, Daten und Geräte und sind in diesem Sinne auch für deren IT-Sicherheit und Schutz verantwortlich.

Alle Nutzerinnen und Nutzer sind in dem für ihre Aufgabe notwendigem Umfang in IT-Sicherheit zu unterrichten. Der IT-Sicherheitsbeauftragte der Max-Planck-Gesellschaft und das Kompetenznetzwerk IT-Sicherheit stellen die dafür nötigen Materialien bereit.

## B. Prozesse der IT-Sicherheit

### 1. Klassifizierung von Daten und Infrastruktur

Jede Einrichtung der Max-Planck-Gesellschaft muss ihre wesentlichen Werte, die für die Arbeit der Einrichtung von Bedeutung sind und eines Schutzes der IT-Sicherheit bedürfen kennen. Dies umfasst z.B. Daten, Anwendungen, Forschungsgeräte, IT-Systeme sowie Netzwerk- und Kommunikationsinfrastruktur. Diese Werte müssen in Bezug auf die klassischen Schutzziele der IT-Sicherheit klassifiziert werden. Diese sind:

- Verfügbarkeit der Informations- und Kommunikationstechnik inklusive der Anwendungen und Daten
- Vertraulichkeit von Daten und Schutz vor unberechtigtem Zugriff
- Integrität der Infrastruktur und der Daten

Um einen adäquaten Schutz erreichen zu können, ist dabei insbesondere die Identifikation der essentiellen Werte der Forschungstätigkeit notwendig.

Dabei soll eine zusammenfassende Klassifikation aller Werte der Einrichtung angestrebt werden. Einzelne Werte, die eines besonderen Schutzes bedürfen, müssen gesondert behandelt werden. Hinweise und Empfehlungen zur Durchführung der Klassifikation finden sich in der "Richtlinie zur Klassifizierung von Werten".

Das Klassifizieren der Daten, Anwendungen und der Infrastruktur ist keine Aufgabe der IT, sondern der Leitung einer Einrichtung, einer Abteilung oder Forschungsgruppe als Eigner der Daten und Anwendungen, da nur diese die Sensibilität beurteilen kann.

Der Klassifizierungsprozess muss in geeigneter Form dokumentiert werden.

## 2. Risikobewertung

Ein systematischer Umgang mit Risiken für die Informationssicherheit dient als Grundlage für die Feststellung des Grades der benötigten IT-Sicherheit sowie zur Planung und Durchführung von Maßnahmen und Aktivitäten im Rahmen der IT-Sicherheit.

Als Basis der Risikobewertung dienen die Klassifizierung von Daten und Infrastrukturen sowie die Identifizierung von Bedrohungen.

Eine regelmäßige Erhebung und Bewertung der IT-Sicherheitsvorfälle in der Max-Planck-Gesellschaft und ihren Einrichtungen ist ein wichtiger Bestandteil der Identifizierung von Bedrohungen. Die Erhebung wird vom Kompetenznetzwerk in Form entsprechender Fragebögen vorbereitet und von der IT-Sicherheitskommission jährlich durchgeführt. Die IT-Sicherheitsbeauftragten der Einrichtungen müssen entsprechende Daten ihrer Einrichtung sammeln und an die IT-Sicherheitskommission übermitteln. Die Resultate der Erhebung bilden die Grundlage des Berichtes der IT-Sicherheitskommission zur Lage der IT-Sicherheit an den Verwaltungsrat der Max-Planck-Gesellschaft und werden in anonymisierter Form allen Einrichtungen zur Verfügung gestellt. Sie dienen den Leitungen und IT-Sicherheitsbeauftragten der Einrichtungen, die Gefährdungslage und damit die Risikobewertung ihrer Einrichtungen neu zu beurteilen.

Um eine bessere Datenbasis für die Risikoermittlung zu erreichen sind Kooperationen mit anderen Forschungsorganisationen und ein gegenseitiger Austausch anonymisierter, statistischer Risikodaten anzustreben.

Die Risikobewertung der Einrichtung muss in geeigneter Form dokumentiert werden.

## 3. IT-Sicherheitskonzept

Jede Einrichtung der Max-Planck-Gesellschaft legt die Maßnahmen und Aktivitäten fest, die notwendig sind, um ihre eigenen und die ihr anvertrauten Werte (Daten, Anwendungen, Infrastruktur aber auch ideelle Werte wie z.B. die Arbeitsfähigkeit oder das Ansehen der Einrichtung und der Max-Planck-Gesellschaft) gegen Gefährdungen zu schützen. Die gewählten Maßnahmen müssen dem Schutzbedarf der Einrichtung angepasst sein, den Stand der Technik berücksichtigen und in einem angemessenen Verhältnis zu der damit angestrebten Risikominderung stehen. Diese Maßnahmen müssen von der Leitung der Einrichtung beschlossen, in einem einrichtungsspezifischen IT-Sicherheitskonzept festgelegt und in angemessener Zeit umgesetzt werden. Das IT-Sicherheitskonzept der Einrichtung, die Umsetzung und die Wirksamkeit der Maßnahmen müssen regelmäßig überprüft, aktualisiert und ggf. einer veränderten Risikobewertung angepasst werden.

Die Max-Planck-Gesellschaft stellt den Einrichtungen einen (elektronischen) Maßnahmenkatalog zur Verfügung, der die möglichen Maßnahmen enthält, die zur Abwehr verschiedener Gefahren und zur Erreichung eines bestimmten IT-Sicherheitslevels dienen. Dieser Maßnahmenkatalog orientiert sich an den DIN ISO/IEC 27001/2-Normen, wird von dem Kompetenznetzwerk IT-Sicherheit erarbeitet und regelmäßig aktualisiert und weiterentwickelt, von der IT-Sicherheitskommission genehmigt und den Einrichtungen zur Realisierung empfohlen. Die einzelnen Einrichtungen können aus diesem Maßnahmenkatalog die für ihre IT-Sicherheitsbedürfnisse angemessenen Maßnahmen übernehmen. Sie können aber auch modifizierte, eigene oder zusätzliche Maßnahmen festlegen.

Einige der Maßnahmen im Maßnahmenkatalog dienen dem Schutz der Max-Planck-Gesellschaft als Ganzes oder sollen Auswirkungen von IT-Sicherheitsvorfällen in einer Einrichtung auf andere ausschließen. Diese Maßnahmen zur Gewährleistung der Rückwirkungsfreiheit werden gesondert in Teil C unter „Mindestanforderungen" aufgeführt und müssen von allen Einrichtungen umgesetzt werden. Über begründete Ausnahmen entscheidet die IT-Sicherheitskommission.

## 4. IT-Sicherheitsvorfälle

Bei einem IT-Sicherheitsvorfall müssen die bzw. der IT-Sicherheitsbeauftragte der Einrichtung und die IT-Leiterin bzw. der IT-Leiter unverzüglich informiert werden. Je nach Schweregrad des Vorfalls ist darüber hinaus auch die Leitung der Einrichtung in Kenntnis zu setzen. Diese entscheidet, ob die bzw. der IT-Sicherheitsbeauftragte der Max-Planck-Gesellschaft und das Kompetenznetzwerk IT-Sicherheit zu informieren sind.

Die bzw. der IT-Sicherheitsbeauftragte der Max-Planck-Gesellschaft und das Kompetenznetzwerk müssen informiert werden, wenn es sich um einen schwerwiegenden Vorfall handelt oder wenn dieser auf andere Einrichtungen Auswirkungen haben könnte. Die bzw. der IT-Sicherheitsbeauftragte der Max-Planck-Gesellschaft entscheidet, ob eine zeitnahe Warnung an alle Einrichtungen ergeht, um diese durch geeignete Maßnahmen zu schützen. Alle IT-Sicherheits-Meldungen werden vertraulich behandelt.

Bei besonders schwerwiegenden Fällen sind auch die IT-Sicherheitskommission und die Präsidentin bzw. der Präsident in Kenntnis zu setzen. Detaillierte Regelungen zur Klassifizierung und Meldung von IT-Sicherheitsvorfällen werden in einem IT-Sicherheitsstandard der Max-Planck-Gesellschaft zum Umgang mit IT-Sicherheitsvorfällen festgelegt, welcher durch die IT-Sicherheitskommission verabschiedet werden muss. Die Leitung der Einrichtung hat entsprechende Regelungen zu treffen, um die Meldung von IT-Sicherheitsvorfällen in ihrem Bereich sicherzustellen.

Alle IT-Sicherheitsvorfälle müssen von den Einrichtungen in geeigneter Form dokumentiert werden.

## 5. Qualitätssicherung

Um Abweichungen festzustellen und die IT-Sicherheit kontinuierlich zu verbessern, sind Methoden und Verfahren zur Qualitätssicherung zu implementieren.

Dokumente zu Prozessen, Verfahren und Maßnahmen im Rahmen der IT-Sicherheit müssen in geeigneter Form erstellt, gepflegt und gegebenenfalls durch die Verantwortlichen freigegeben werden, um eine effektive Planung, Durchführung und Kontrolle der IT-Sicherheit zu gewährleisten. Die Dokumentation sollte regelmäßig überprüft und aktualisiert sowie über geeignete Kanäle an alle Betroffenen kommuniziert werden.

Um die IT-Sicherheit kontinuierlich zu verbessern, bedarf es insbesondere Monitoring-Maßnahmen, interner Überprüfungen und auch Audits durch Dritte (z.B. durch andere Einrichtungen oder Dienstleister).

## C. Mindestanforderungen

### 1. Organisation

Die Leitung der Einrichtung muss eine Person als IT-Sicherheitsbeauftragte bzw. IT-Sicherheitsbeauftragten benennen.

Die Einrichtung muss in angemessener Zeit ein einrichtungsspezifisches IT-Sicherheitskonzept auf Basis dieser IT-Sicherheitsrichtlinie entwickeln und in Kraft setzen.

### 2. Nutzerverwaltung und Nutzungsordnung

Die Einrichtung muss einen kontrollierten Prozess zur Benutzerverwaltung etablieren. Insbesondere die Erteilung von Sonderzugangsrechten muss klar geregelt und entsprechend dokumentiert werden.

Die Einrichtung muss die Rechte und Pflichten der Nutzerinnen und Nutzer der IT-Infrastruktur in einer Nutzungsordnung regeln und muss sicherstellen, dass alle Nutzerinnen und Nutzer davon Kenntnis erlangen. Insbesondere muss darin den Nutzerinnen und Nutzern ihre Rolle und Verantwortlichkeit für die IT-Sicherheit bewusstgemacht werden.

### 3. Physische IT-Sicherheit

Die Einrichtung muss die Sicherheitsbereiche festlegen, in denen besonders schutzwürdige IT-Infrastruktur (Server, Netzwerkkomponenten, Datenträger, TK-Anlagen, u.ä.) aufgestellt ist, und den Zutritt zu diesen Bereichen regeln. Es sind geeignete Maßnahmen zu ergreifen, um den Zutritt ausschließlich auf berechtigte Personen zu beschränken.

### 4. Netzwerk

Die Einrichtung muss die Zuständigkeiten und Verfahren für die Verwaltung und Kontrolle seines Netzwerks regeln.

Das Netz einer Einrichtung ist durch technisch aktuell gehaltene Firewall-Technologien zumindest gegenüber dem Internet abzusichern. Je nach Schutzbedarf muss das Netz gegebenenfalls in separate Netzwerkdomänen unterteilt und die domänenübergreifenden Zugriffe abgesichert werden. Von außen eingehende Verbindungen sind nur zu freigegebenen Servern zulässig.

Der Zugriff von außen auf nicht öffentliche Ressourcen der Einrichtung muss zwingend durch verschlüsselte und zugangskontrollierte Zugriffsmöglichkeiten geschützt werden.

Der Zugriff auf öffentliche Ressourcen muss soweit technisch sinnvoll auch verschlüsselt ermöglicht werden.

Alle aktiven Netzwerkkomponenten sind vor unberechtigtem Zutritt und Zugang zu sichern.

### 5. Backup

Die Einrichtung muss ein Datensicherungskonzept erstellen, dokumentieren und realisieren, das dem IT-Sicherheitsbedürfnis der Einrichtung entspricht. Hierbei sind insbesondere

der Standort der Sicherungsmedien und die Überprüfung der Funktionsfähigkeit der Wiederherstellung zu regeln.

## 6. Archivierung

Gemäß den „Regeln zur Sicherung guter wissenschaftlicher Praxis" muss die Einrichtung Maßnahmen ergreifen, um elektronische Aufzeichnungen ihrer wissenschaftlichen Tätigkeit vor Verlust, Zerstörung oder Fälschung zu sichern und über einen längeren Zeitraum aufzubewahren. Entsprechende Verfahren unter Nutzung eigener oder zentral bereitgestellter technischer Möglichkeiten zur Archivierung müssen aufgestellt werden.

## 7. Patchmanagement

Die Einrichtung muss die technischen Schwachstellen seiner IT-Infrastruktur regelmäßig überprüfen und geeignete Maßnahmen für den Umgang mit den daraus resultierenden Risiken ergreifen. Diese sind entsprechend zu dokumentieren. Insbesondere ist der Umgang mit Sicherheitspatches zu regeln.

## 8. Schadsoftware

Jede Einrichtung der Max-Planck-Gesellschaft muss ein dokumentiertes Schutzkonzept vor Schadsoftware haben.

Auf virengefährdeten Betriebssystemen muss eine Software eingesetzt werden, die Schadsoftware erkennt und wenn möglich entfernt. Wenn dies nicht möglich ist, müssen andere Maßnahmen zur Risikominimierung eingesetzt werden. Die Software muss regelmäßig aktualisiert werden, um auch neue Versionen von Schadsoftware erkennen und behandeln zu können.

## 9. E-Mail

Eingehende E-Mails müssen auf Schadsoftware und auf SPAM untersucht werden. Zusätzlich müssen Maßnahmen ergriffen werden, um den Versand von Schadsoftware und SPAM zu unterbinden.

## 10. Vertrauliche Daten

Vertrauliche Daten müssen durch Verschlüsselung geschützt werden, wenn eine der folgenden Bedingungen vorliegt:

- sie werden per E-Mail verschickt
- sie werden auf mobilen Datenträgern gespeichert
- sie werden auf Servern bei einem externen Dienstleister gespeichert (z.B. in der Cloud)
- ein externer Dienstleister hat Zugriff auf intern gespeicherte Daten

Sofern eine Verschlüsselung bei einem Dienstleister technisch nicht möglich ist, müssen vertragliche Regelungen mit dem Dienstleister die Vertraulichkeitsanforderungen beim Speichern und Verarbeiten organisatorisch sicherstellen.

Es sind geeignete Maßnahmen für das Schlüsselmanagement zu ergreifen.