IT-Sicherheitsleitlinie der Max-Planck-Gesellschaft

Am 21.06.2017 vom Verwaltungsrat beschlossen

Präambel

Die Max-Planck-Gesellschaft ist für die Erfüllung ihrer Aufgaben auf eine zuverlässig funktionierende Informations- und Kommunikationstechnik angewiesen. Wissenschaftliche Forschung erfordert darüber hinaus ein hohes und ihrem jeweiligen Forschungsbereich entsprechendes Maß an Sicherheit und Integrität ihrer Daten. Es ist daher unerlässlich, umfassende Maßnahmen zum Schutz von Infrastruktur und Daten zu ergreifen.

Der sichere Umgang mit Informationen ist für die Max-Planck-Gesellschaft von essentieller Bedeutung. Das macht die IT-Sicherheit zum Schutz ihrer Infrastrukturen und Daten zu einem wesentlichen Ziel.

Dieses Dokument definiert die IT-Sicherheitsleitlinie für die Max-Planck-Gesellschaft. Es stellt die Basis für eine IT-Sicherheitsrichtlinie und daraus folgende Maßnahmen für eine stetige Verbesserung und dauerhafte Aufrechterhaltung der Sicherheit im Bereich der Informations- und Kommunikationstechnik (IT) dar.

Das Spektrum der IT-Anwendungen in der Max-Planck-Gesellschaft umfasst wissenschaftliche Anwendungen und Simulationen, die Durchführung von Versuchen und Experimenten, die Präsentation wissenschaftlicher Ergebnisse, Büroanwendungen, die Arbeit der Verwaltungen, die Steuerung und den Betrieb technischer Anlagen sowie die Kommunikation mit internen sowie externen Partnern.

Die Diversität der Forschungsgebiete, eines der wesentlichen Merkmale der Max-Planck-Gesellschaft, spiegelt sich in ihren Methoden, Werkzeugen und dem Schutzbedarf ihrer Einrichtungen wider, was die Anforderungen an die jeweilige IT-Infrastruktur stark prägt. Dementsprechend sind die Auswirkungen von Störungen oder Ausfällen in den verschiedenen Anwendungsgebieten auch von unterschiedlicher Tragweite. Gleiches gilt auch für die IT-Sicherheitsmaßnahmen.

Zielsetzungen

Die Max-Planck-Gesellschaft schützt ihre Interessen und ihr Ansehen in der Öffentlichkeit durch die Sicherung ihrer Arbeitsfähigkeit, Vertrauenswürdigkeit und Zuverlässigkeit für ihre Kooperationspartner. Zu ihren IT-Sicherheitszielen zählen:

- Gewährleistung der Verfügbarkeit der IT-Systeme, Anwendungen und Daten.
- Erhalt der Integrität der IT-Systeme, Anwendungen und Daten.
- Erhalt der Vertraulichkeit von Daten
- Verhinderung missbräuchlicher Nutzung der IT-Systeme, Anwendungen und Daten (zweckwidrige Nutzung, Nutzung durch Unbefugte), sowohl aus Gründen des Selbstschutzes als auch zum Schutze Dritter.
- Einhaltung gesetzlicher Regelungen, Vorgaben der Zuwendungsgeber oder vertraglicher Verpflichtungen bezüglich der Informationssicherheit.
- Wahrung der Persönlichkeitsrechte der Mitarbeiterinnen und Mitarbeiter sowie aller in sonstigen Beziehungen zur Max-Planck-Gesellschaft stehenden Personen.

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.

Wegen der sich stetig ändernden Gefahren, Anforderungen und neuen technischen Möglichkeiten sind die Aufrechterhaltung und die Verbesserung der IT-Sicherheit eine permanente Aufgabe, die in ständigen Prozessen eine stetige Weiterentwicklung auf allen beteiligten Ebenen anstreben muss. Dies erfordert neben der Mitwirkung jeder bzw. jedes Einzelnen sowohl personelle als auch finanzielle Mittel.

Verantwortlichkeiten

Der Verwaltungsrat und die Leitungen aller Einrichtungen des Max-Planck-Gesellschaft e.V. (Institute, Forschungsstellen, Generalverwaltung und zentrale Einrichtungen) sowie Mitarbeiterinnen und Mitarbeiter und Nutzerinnen und Nutzer der IT-Infrastruktur der Max-Planck-Gesellschaft tragen durch ihr Verhalten zur Gewährleistung der IT-Sicherheit in der Max-Planck-Gesellschaft bei. Der Verwaltungsrat erwartet, dass auch die Leitungen der rechtlich selbständigen Einrichtungen der Max-Planck-Gesellschaft dieser Verantwortung gerecht werden und unter Berücksichtigung der individuellen Situation über entsprechende Regelungen verfügen. Aufgrund der dezentralen Strukturen der Max-Planck-Gesellschaft und der kollaborativen und mobilen Arbeitsweise in der Wissenschaft kommt den Leitungen der Max-Planck-Institute und ihren wissenschaftlichen Mitarbeiterinnen und Mitarbeitern eine wichtige Rolle bei der Erreichung der Ziele zu.

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 neben dieser IT-Sicherheitsleitlinie der Max-Planck-Gesellschaft die IT-Sicherheitsrichtlinie der Max-Planck-Gesellschaft mit weitergehenden organisatorischen, prozessualen und technischen Regelungen. Angesichts der Veränderungsgeschwindigkeit in Fragen der IT-Sicherheit soll die IT-Sicherheitsrichtlinie der Max-Planck-Gesellschaft aber auch ein Verfahren vorsehen, das notwendige Anpassungen der Vorgaben zum Mindestschutz durch die IT-Sicherheitskommission mit einer erst nachlaufenden Befassung durch den Verwaltungsrat ermöglicht.

Die **IT-Sicherheitskommission der Max-Planck-Gesellschaft** ist ein ständiges von der Präsidentin bzw. dem Präsidenten der Max-Planck-Gesellschaft eingesetztes Gremium unter der Leitung einer Vizepräsidentin bzw. eines Vizepräsidenten der Max-Planck-Gesellschaft. Sie initiiert und koordiniert alle mit der IT-Sicherheit verbundenen Aktivitäten.

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 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.

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 Sicherheitsniveau und schafft die erforderlichen Rahmenbedingungen, um der IT-Sicherheit in ihrem Zuständigkeitsbereich den erforderlichen Stellenwert zu geben. Sie stellt die notwendigen Ressourcen für die Erreichung der Sicherheitsziele zur Verfügung.

Jede Nutzerin und jeder Nutzer der Informations- und Kommunikationstechnik ist für die Sicherheit und den Schutz der Daten in ihrem bzw. seinem Verantwortungsbereich verantwortlich. Sie bzw. er ist verpflichtet, bei der Erfüllung der Aufgabe „IT-Sicherheit" kooperativ und verantwortungsbewusst mitzuwirken.