Universität Rostock Traditio et Innovatio

Amtliche Bekanntmachungen

Jahrgang 2017 Nr. 8 Rostock, 10.03.2017

Leitlinie zur Gewährleistung der IT-Sicherheit an der Universität Rostock - IT-Sicherheitsleitlinie - vom 9. März 2017

HERAUSGEBER
DER REKTOR DER UNIVERSITÄT ROSTOCK
18051 ROSTOCK

Universität Rostock Traditio et Innovatio

Leitlinie zur Gewährleistung der IT-Sicherheit an der Universität Rostock

- IT-Sicherheitsleitlinie -

Beschlossen vom Rektorat am 6. März 2017

Inhaltsverzeichnis:

Präambel

Die Universität Rostock ist in Hinblick auf eine leistungs- und zukunftsfähige Forschung, Lehre und Verwaltung auf sichere und funktionierende Informations- und Kommunikationstechnologien (IKT) angewiesen.

Immer mehr Abläufe und Mechanismen sind im hohen und zunehmenden Maße von modernen IKT abhängig, sodass umfangreiche Schutzmaßnahmen in Bezug auf die Verfügbarkeit, Integrität und Vertraulichkeit der zu verarbeitenden Daten und Informationen zu ergreifen sind. In diesem Zusammenhang erfolgt eine Orientierung an den Empfehlungen, Vorschlägen und Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie der internationalen Normenreihe ISO/IEC 27000.

Die IT-Sicherheit erfüllt keinen Selbstzweck. Folglich ist der Einsatz von Schutzmaßnahmen stets in Relation zum erzielten Sicherheitsgewinn zu setzen. Hierdurch wird gewährleistet, dass ein Streben nach Sicherheit und die Freiheit von Forschung und Lehre miteinander vereinbar sind.

Die IT-Sicherheitsleitlinie beschreibt den Informationssicherheitsprozess und gilt als wichtiges Grundsatzdokument in Hinblick auf den Stellenwert, die verbindlichen Prinzipien und das anzustrebende Niveau der Informationssicherheit an der Universität Rostock. Im Fokus stehen hierbei die zu erreichenden Sicherheitsziele sowie die damit einhergehenden organisatorischen Rahmenbedingungen zur Erreichung dieser Ziele. Die IT-Sicherheitsleitlinie dient als Grundlage für ein einheitliches IT-Sicherheitskonzept.

Das Rektorat setzt die IT-Sicherheitsleitlinie in Kraft und trägt die Gesamtverantwortung für die IT-Sicherheit an der Universität Rostock. Dementsprechend steht er in vollem Umfang hinter den in der Leitlinie formulierten Zielen und den daraus abgeleiteten und abzuleitenden Konzepten und Maßnahmen.

Eine erfolgreiche Umsetzung des Informationssicherheitsprozesses setzt die Unterstützung aller Mitglieder der Universität Rostock voraus.

1 Geltungsbereich

Die in der IT-Sicherheitsleitlinie beschriebenen personellen, organisatorischen, technischen und infrastrukturellen Maßnahmen sind nach Inkraftsetzung durch das Rektorat für alle Mitglieder der Universität Rostock verbindlich zu beachten und einzuhalten.

Des Weiteren gilt die IT-Sicherheitsleitlinie für alle Einrichtungen der Universität Rostock, einschließlich der gesamten IT-Infrastruktur, den betriebenen IT-Systemen sowie allen am Netzwerkverbund angeschlossenen Geräten. Dies beinhaltet sowohl die Planung als auch den operativen Betrieb der IKT.

Für externe Nutzende bzw. bei vertraglichen Beziehungen mit Dritten gilt die IT-Sicherheitsrichtlinie äquivalent.

2 Ziele der IT-Sicherheit

Zum Schutz der Infrastruktur, Systeme, Anwendungen, Informationen und Daten an der Universität Rostock ist ein angemessenes Schutzniveau im jeweils erforderlichen und wirtschaftlichen Maße herzustellen und zu bewahren. Das Schutzniveau basiert primär auf den anzustrebenden Schutzzielen: Verfügbarkeit, Vertraulichkeit und Integrität. In diesem Zusammenhang gilt es ermittelte Risiken durch angemessene Maßnahmen auf ein akzeptierbares Maß zu reduzieren.

2.1 Verfügbarkeit

Die Verfügbarkeit von informationstechnologischer Infrastruktur, Systemen, Anwendungen und Netzen wird gewährleistet, wenn diese zeitgerecht zur Verfügung stehen und auf die Daten wie vorgesehen zugegriffen werden kann. Hierbei geht es um das Verhältnis (in Prozent) der Zeit, in der die IKT tatsächlichen verfügbar war (Betriebszeit), gemessen am vorab definierten Gesamtzeitraum. Die jederzeitige Verfügbarkeit (100 Prozent) bildet demzufolge den Idealzustand. Bei fehlender Verfügbarkeit handelt es sich um eine Ausfallzeit. Für kritische Bereiche lässt sich das Verfügbarkeitslevel u. a. durch den Einsatz von redundanten Systemen und Notstromversorgungseinrichtungen erhöhen.

2.2 Vertraulichkeit

Die Vertraulichkeit wird gewährleistet, wenn schützenswerte Daten und Informationen nur den hierfür berechtigten Personen zugänglich gemacht werden. Demzufolge wird der Personenkreis mittels Maßnahmen zum Zugangs- und Zugriffsschutz (z. B. durch Berechtigungen) eingeschränkt. Dies gilt sowohl räumlich als auch bezogen auf das jeweilige IT-System. Ein weiteres Instrument zum Schutz der Vertraulichkeit für die Speicherung und den Transport von Daten stellt die symmetrische/ asymmetrische Verschlüsselung dar. Unautorisierte Dritte sind hierbei nicht in der Lage, die transformierten Daten zu interpretieren.

2.3 Integrität

Die Integrität (Unversehrtheit) wird gewährleistet, wenn einerseits schützenswerte Daten korrekt (unverfälscht) und vollständig (unbeschädigt) sind und andererseits IKT in ihrer Funktion korrekt funktionieren. Verfälschungs- und Beschädigungsmöglichkeiten ergeben sich aus dem Löschen, Ersetzen bzw. Hinzufügen von Daten. Unautorisierte Manipulationen gilt es dementsprechend mittels technischen und organisatorischen Sicherheitsmaßnahmen entgegenzuwirken. Geeignete Maßnahmen bilden hierbei u. a. der Einsatz von elektronischen Signaturen und Zertifikaten.

3 Prinzipien und Grundsätze der IT-Sicherheit

Für die Erstellung von IT- und IT-Sicherheitskonzepten sowie den sich hieraus abzuleitenden Maßnahmen sind nachfolgende Prinzipien und Grundsätze zu berücksichtigen.

3.1 Angemessenheit von IT-Sicherheitsmaßnahmen

Die zu erreichenden Ziele und der ermittelte Aufwand von IT-Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zueinander stehen. Unter Beachtung der gesetzlich vorgeschriebenen IT-Sicherheitsanforderungen und den sich hieraus ergebenden IT-Sicherheitsmaßnahmen muss zudem stets das Verhältnis zum Schutzzweck mit Blick auf die Angemessenheit überprüft werden. Dabei ist darauf zu achten, dass IT-Sicherheitsmaßnahmen die bestehenden Abläufe und Prozesse so gering wie möglich beeinträchtigen. Unumgänglich notwendige IT-Sicherheitsmaßnahmen werden auch dann ergriffen, wenn ein Einsatz von IKT hierdurch erschwert wird.

3.2 Bereitstellung von ausreichenden Ressourcen für die IT-Sicherheit

Die Universität Rostock stellt ausreichende finanzielle, personelle sowie zeitliche Ressourcen zur Erreichung und Aufrechterhaltung eines angemessenen IT-Sicherheitsniveaus bereit. Mittel zur Pflege, Wartung und zyklischen Erneuerung sind hierbei zu berücksichtigen.

Es ist darauf zu achten, dass die standardmäßigen IT-Sicherheitsmaßnahmen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Daten, Informationen und Systeme stehen. Dieser Wert wird u. a. durch die Höhe von möglichen finanziellen Schäden, dem Einwirken auf das Recht auf informationelle Selbstbestimmung, durch die Folgen von Gesetzesverstößen oder durch eine Beschädigung der Reputation der Universität Rostock bestimmt. Dementsprechende Schäden mit hohen finanziellen Auswirkungen gilt es unabdingbar zu verhindern.

3.3 Einbindung aller Mitglieder in den Informationssicherheitsprozess

IT-Sicherheit betrifft ausnahmslos alle Mitglieder der Universität Rostock. Mit Hilfe eines verantwortungs- und sicherheitsbewussten Handelns durch jede einzelne Person wird es möglich, Schadensfälle auf ein Minimum zu reduzieren und den Informationssicherheitsprozess nach besten Kräften zu unterstützen. Diesbezüglich gilt es alle Mitglieder der Universität Rostock im erforderlichen Umfang zu informieren, zu sensibilisieren und zu qualifizieren.

Es empfiehlt sich über den Sinn und den Zweck einer IT-Sicherheitsmaßnahme mit entsprechend großen Auswirkungen auf die Mitglieder der Universität Rostock in angemessener Weise aufzuklären, solange sich daraus kein Sicherheitsrisiko ergibt. Somit wird ein höchstmögliches Maß an Transparenz und Verständlichkeit erzeugt. Dies gilt insbesondere bei Einschränkungen im Funktions- und Komfortumfang.

3.4 Schutzbedarfsfeststellung

Der Schutzbedarf orientiert sich an den möglichen Schäden, die mit einer Beeinträchtigung von betroffenen Daten, Informationen, Systemen und den damit verknüpften Abläufen einhergehen. Das Ziel ist hierbei, den jeweiligen Schutzbedarf in Hinblick auf die Verfügbarkeit, Vertraulichkeit und Integrität zu ermitteln. Da der Schutzbedarf zumeist nicht quantifizierbar ist, erfolgt eine qualitative Bewertung auf Basis von drei Schutzbedarfskategorien (normal, hoch, sehr hoch).

Liegt ein normaler Schutzbedarf vor, sind die vorgesehenen IT-Sicherheitsmaßnahmen der aufgeführten Regelwerke und Normen umzusetzen. Liegt ein hoher bzw. sehr hoher Schutzbedarf vor, muss eine ergänzende Sicherheitsanalyse durchgeführt werden. Die sich hieraus ergebenen zusätzlichen IT-Sicherheitsmaßnahmen sind dementsprechend zu berücksichtigen.

Für alle IT-Systeme, IT-Verfahren, IT-Anwendungen und Informationen der Universität Rostock ist eine Person sowie ein Vertreter zu benennen, der den jeweiligen Schutzbedarf bestimmt und die dazugehörigen Zugriffsberechtigungen erteilt und dokumentiert.

3.5 Umgang mit datenschutzrechtlichen Bestimmungen

Für die Universität Rostock gelten die gesetzlichen Bestimmungen des Bundesdatenschutzgesetzes (BDSG) sowie das Gesetz zum Schutz des Bürgers bei der Verarbeitung seiner Daten für das Bundesland Mecklenburg-Vorpommern in der jeweils gültigen Fassung. Zudem ist die EU-Datenschutz-Grundverordnung (EU-DSGVO) ab dem 25.05.2018 verbindlich anzuwenden. Für die Universität Rostock hat der Schutz von personenbezogenen Daten oberste Priorität. Dies betrifft insbesondere die Datenbestände aus Verwaltung, Forschung und Lehre.

4 IT-Sicherheitsmaßnahmen

Nachfolgende IT-Sicherheitsmaßnahmen bilden übergreifende Aspekte zur Aufrechterhaltung und Steigerung des IT-Sicherheitsniveaus an der Universität Rostock.

4.1 Verpflichtung zur Einhaltung der IT-Sicherheit

Alle Mitglieder der Universität Rostock verpflichten sich zur Gewährleistung der IT-Sicherheit durch ein verantwortungsvolles Handeln. Zudem halten Sie die für die IT-Sicherheit relevanten Gesetze, Richtlinien, Vorschriften, Anweisungen und Regelungen ein. Für ein kontinuierliches Informationsmanagement, Fortbildungen und Sensibilisierungsmaßnahmen sind entsprechende Ressourcen einzuplanen.

4.2 IT-Sicherheitskonzept

Für die Universität Rostock ist ein IT-Sicherheitskonzept zu erstellen und aktuell zu halten. Es umfasst alle IT-Systeme und -verfahren einschließlich der jeweiligen Schutzbedarfsfeststellung und beschreibt die für einen definierten Bereich notwendigen Maßnahmen zur Erreichung der jeweiligen Schutzziele.

Somit werden alle spezifischen Gefahren aufgelistet und entsprechende Schritte zur Risikominimierung beschrieben.

4.3 Berichts- und Informationswesen

Zum jeweils abgeschlossenen Quartal erstellt die IT-Sicherheitsbeauftragte bzw. der IT-Sicherheitsbeauftragte dem Rektorat einen Bericht über die Vollständigkeit, Aktualität und den Umsetzungsstand des IT-Sicherheitskonzepts.

IT-Sicherheitsvorfälle sind zu erfassen und im jeweiligen Quartalsbericht aufzuführen. Ein Sicherheitsvorfall ist jedes Ereignis, dass die IT-Sicherheit beeinträchtigt und in der Konsequenz Schäden nach sich ziehen kann. IT-Sicherheitsvorfälle mit einem beträchtlich anzunehmenden Ausmaß sind umgehend an das Rektorat zu melden.

Mit Hilfe von IT-Sicherheitsweisungen und IT-Sicherheitsmitteilungen werden alle Mitglieder der Universität Rostock entsprechend den aktuellen Gegebenheiten und den einzuhaltenden Bestimmungen informiert.

4.4 Notfallmanagement

Um größere Schäden in Folge von Notfällen zu begrenzen bzw. diesen vorzubeugen, muss auf IT-Sicherheitsvorfälle zügig und konsequent reagiert werden. Bei einem Systemausfall sind kritische Bereiche und Abläufe aufrecht zu erhalten und die Verfügbarkeit der ausgefallenen Systeme innerhalb einer tolerierbaren Zeitspanne wiederherzustellen.

Maßnahmen für den Notfall werden in einem separaten Notfallhandbuch zusammengestellt.

4.5 Übungen, Kontrollen und der Umgang mit IT-Sicherheitsverstößen

Mit Hilfe von IT-Sicherheits- und Krisenmanagementübungen sind bestimmte Bereiche, Abläufe und IKT der Universität Rostock anhand praxisnaher Szenarien kontinuierlich zu überprüfen. Hierbei ist es das Ziel, die Mitglieder der Universität Rostock für einzelne Themenbereiche der IT-Sicherheit zu sensibilisieren, die Zusammenarbeit von einzelnen Akteuren an der Universität Rostock zu verbessern sowie das IT-Sicherheitsniveau der Universität Rostock kontinuierlich zu steigern und dauerhaft zu gewährleisten.

Um ein möglichst unverzerrtes Lagebild hinsichtlich der IT-Sicherheit an der Universität Rostock zu erhalten, können gelegentlich auch unangekündigte Kontrollen durchgeführt werden. Es ist nicht das Ziel einer Person professoral gegenüberzutreten oder diese als „Schuldige“ bzw. „Schuldigen“ zu

identifizieren, sondern vielmehr auf qualifizierter Weise Mängel aufzuzeigen und diesbezügliche Lösungsmöglichkeiten anzubieten.

Jegliche Verstöße in Hinblick auf die IT-Sicherheit an der Universität Rostock sind den zuständigen Stellen unverzüglich zu melden. Verhalten, dass die Sicherheit von Daten, Informationen, IT-Systemen oder Netze gefährdet, kann disziplinar- oder arbeitsrechtlich geahndet werden. Unter bestimmten Umständen kann dementsprechendes Verhalten als Ordnungswidrigkeit oder Straftat verfolgt werden.

4.6 Zugangs- und Zugriffsschutz

Die Gebäude und Räumlichkeiten der Universität Rostock werden durch Zutrittskontrollen bzw. Zutrittskontrollsysteme geschützt. Für die IT-Betriebs- und IT-Verteilerräume besteht ein erhöhter Schutzbedarf, sodass der Zutritt sowie der Zugang durch ein restriktives Berechtigungskonzept zu schützen ist.

Der Zugriff auf IKT ist zwingend auf den minimal erforderlichen Personenkreis zu beschränken. Hierbei gilt es zu beachten, dass Zugriffsberechtigungen ausschließlich zur Aufgabenerfüllung erteilt werden. Für jedes IT-System bzw. -verfahren sind die Zugriffsberechtigungen zu dokumentieren und kontinuierlich zu überprüfen.

4.7 Datensicherung

Durch eine möglichst allumfassende Datensicherung wird gewährleistet, dass der Grundbetrieb nach einem Datenverlust in kurzer Zeit wiederaufgenommen werden kann. Dies gilt insbesondere dann, wenn Teile des operativen Datenbestandes verloren gehen oder offensichtlich fehlerhaft sind. Informationen werden einheitlich gekennzeichnet und so aufbewahrt, dass sie schnell auffindbar sind.

5 IT-Sicherheitsorganisation

Das Rektorat trägt die Gesamtverantwortung für eine angemessene IT-Sicherheit an der Universität Rostock und stellt die erforderlichen personellen und finanziellen Ressourcen für die Einrichtung der nachfolgenden Instanzen der IT-Sicherheitsorganisation zur Verfügung.

5.1 IT-Sicherheitsbeauftragte bzw. IT-Sicherheitsbeauftragter

Für die Universität Rostock ist durch die Rektorin bzw. den Rektor eine fachlich qualifizierte IT-Sicherheitsbeauftragte bzw. eine fachlich qualifizierter IT-Sicherheitsbeauftragter sowie eine Stellvertreterin bzw. ein Stellvertreter zu benennen. Diesbezüglich werden folgende Aufgaben übertragen:

- Steuerung des Informationssicherheitsprozesses sowie Mitwirkung bei allen damit verbundenen Aufgaben,
- Konzeptionierung, Realisierung, Überprüfung und kontinuierliche Fortschreibung der Vorgaben, Richtlinien und Regelungen zur IT-Sicherheit an der Universität Rostock,
- Koordinierung von Maßnahmen zur Steigerung des IT-Sicherheitsniveaus an der Universität Rostock,
- Beratung und Sensibilisierung der Studentinnen und Studenten, Mitarbeiterinnen und Mitarbeiter sowie Führungskräfte zu einem verantwortungsvollen Umgang mit IKT,
- Koordinierung von Sensibilisierungs- und Schulungsmaßnahmen zum Thema IT-Sicherheit,

- regelmäßige Teilnahme an Informations- und Fortbildungsmaßnahmen mit Bezug zum Thema IT-Sicherheit

Darüber hinaus werden folgende Befugnisse und Kompetenzen erteilt:

- Ansprechpartnerin bzw. Ansprechpartner in allen Fragen der IT-Sicherheit an der Universität Rostock,
- Untersuchungsinstanz bei sicherheitsrelevanten Vorfällen in Zusammenhang mit IKT,
- Vorsitzende bzw. Vorsitzender des IT-Sicherheitsmanagementteams,

Die IT-Sicherheitsbeauftragte bzw. der IT-Sicherheitsbeauftragte ist in ihrer bzw. seiner Funktion organisatorisch direkt der Rektorin bzw. dem Rektor unterstellt. Er meldet anlassbezogene Vorkommnisse und Informationen direkt an die Rektorin bzw. den Rektor. Zudem erstellt sie bzw. er für jedes abgeschlossene Quartal einen Bericht zum Stand der IT-Sicherheit an der Universität Rostock und übermittelt diesen an das Rektorat.

Die IT-Sicherheitsbeauftragte bzw. der IT-Sicherheitsbeauftragte ist bei ihrer bzw. seiner Arbeit durch alle Mitglieder der Universität Rostock sowie insbesondere durch die IT-Organisation der Universität Rostock zu unterstützen. Sie bzw. er arbeitet mit der Leitungsinstanz des IT- und Medienzentrums (ITMZ), der Datenschutzbeauftragten bzw. dem Datenschutzbeauftragten sowie weiteren Beauftragten mit Bezug zu sicherheitsrelevanten Themen konstruktiv und vertrauensvoll zusammen. Gegenüber den IT-Verantwortlichen, den System- und Anwendungsbetreuerinnen bzw. System- und Anwendungsbetreuern sowie den IT-Nutzerinnen und IT-Nutzer besteht in Hinblick auf die IT-Sicherheit Weisungsbefugnis.

Um bereits in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen sowie spezifische Methoden und Prozesse für die IT-Sicherheit zu vereinbaren, ist die IT-Sicherheitsbeauftragte bzw. der IT-Sicherheitsbeauftragte frühzeitig in alle Projekte der Universität Rostock mit Bezug zu IKT unaufgefordert zu beteiligen und einzubinden. Dies gilt insbesondere für die Erarbeitung von Vorgaben für zu beschaffene Hard- und Software.

Bei Gefahr in Verzug sowie bei zu befürchtenden gravierenden Schäden für die IT-Infrastruktur veranlasst die IT-Sicherheitsbeauftragte bzw. der IT-Sicherheitsbeauftragte gemeinsam mit der Leitungsinstanz des ITMZ Sofortmaßnahmen zur Sicherung der betroffenen IT-Systeme, IT-Verfahren oder Netze, beispielweise durch Stilllegung oder den Zugriff auf notwendige Informationen innerhalb des Systems. Das Rektorat ist in diesem Fall umgehend zu informieren.

Weitere Einzelheiten werden in der Bestellung zur bzw. zum IT-Sicherheitsbeauftragten geregelt.

5.2 IT-Sicherheitsmanagementteam

Das IT-Sicherheitsmanagementteam berät und unterstützt die IT-Sicherheitsbeauftragte bzw. den IT-Sicherheitsbeauftragten bei der Konzeptionierung, Realisierung, Dokumentation und Kontrolle der im Rahmen des Informationssicherheitsprozesses zu erstellenden Dokumente. Zudem kann das IT-Sicherheitsmanagementteam bei einem zu befürchtenden oder eingetretenen IT-Sicherheitsvorfall einberufen werden.

Das IT-Sicherheitsmanagementteam setzt sich aus mindestens einer Vertreterin bzw. einem Vertreter der nachfolgenden Organisationsbereiche zusammen, wobei die bzw. der IT-Sicherheitsbeauftragte den Vorsitz führt:

- IT-Sicherheitsbeauftragte bzw. IT-Sicherheitsbeauftragter
- IT- und Medienzentrum - Abteilung Netzdienste und Medienservice
- IT- und Medienzentrum - Abteilung Systeme und Dienste
- IT- und Medienzentrum - Abteilung Anwendungen und Medien

- IT- und Medienzentrum - Abteilung Campus- und Verwaltungssysteme
- IT- und Medienzentrum - Leitungsinstanz (bei Bedarf)
- Datenschutzbeauftragte bzw. Datenschutzbeauftragter (bei Bedarf)
- Referat Betriebstechnik und Logistik (D3.3) (bei Bedarf)

Weitere Personen (z. B. aus universitären Einrichtungen oder Fakultäten bzw. externen Stellen) können auf Einladung durch die IT-Sicherheitsbeauftragte bzw. den IT-Sicherheitsbeauftragten beratend hinzugezogen werden.

5.3 Ansprechpartnerin bzw. Ansprechpartner IT-Sicherheit

Jede zentrale Einrichtung und Fakultät der Universität Rostock benennt eine Person, die aufgrund ihrer Position oder beruflichen Erfahrung der IT-Sicherheitsbeauftragten bzw. dem IT-Sicherheitsbeauftragten als Ansprechpartnerin bzw. Ansprechpartner zur Thematik „IT-Sicherheit“ dient.

5.4 IT-Nutzerinnen und IT-Nutzer

Alle Mitglieder der Universität Rostock unterstützen die IT-Sicherheitsbeauftragte bzw. den IT-Sicherheitsbeauftragten in ihrer bzw. seiner Arbeit vollumfänglich nach bestem Wissen und Gewissen. Dementsprechend gilt es sich in Hinblick auf sicherheitsrelevante Fragestellungen an die Anweisungen der IT-Sicherheitsbeauftragten bzw. des IT-Sicherheitsbeauftragten zu halten. Sicherheitsrelevante Vorfälle mit Bezug auf IKT sind unverzüglich an die IT-Sicherheitsbeauftragte bzw. den IT-Sicherheitsbeauftragten

Telefon: +49 (0) 381 498 **3350**
E-Mail: it-sicherheit@uni-rostock.de

oder im Notfall an den Dispatcherdienst Technik, Bau und Liegenschaften (D3.3.3)

Telefon: +49 (0) 381 498 **1111**

zu melden.

6 Schlussbestimmung

Der Informationssicherheitsprozess ist kontinuierlich auf seine Wirksamkeit sowie Aktualität zu kontrollieren. IT-Sicherheitsmaßnahmen sind regelmäßig dahingehend zu überprüfen, inwiefern diese auch weiterhin umsetzbar und den betroffenen Mitgliedern der Universität Rostock bekannt sind.

Alle Mitglieder der Universität Rostock werden ermutigt, Schwachstellen und mögliche Optimierungspotentiale direkt an die IT-Sicherheitsbeauftragte bzw. den IT-Sicherheitsbeauftragten weiterzuleiten. Das Rektorat unterstützt die kontinuierliche Steigerung des IT-Sicherheitsniveaus mit Nachdruck.

Die IT-Sicherheitsleitlinie tritt mit der Amtlichen Bekanntmachung in Kraft.

Rostock, 9. März 2017

Prof. Dr. med. Wolfgang Schareck

Rektor