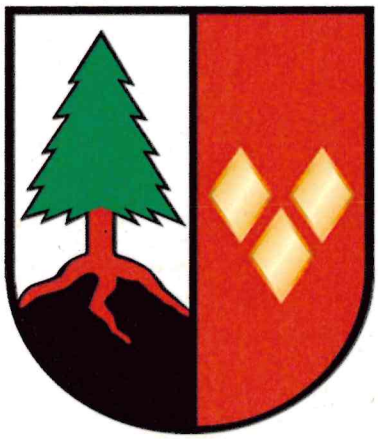
Stand: 29.09.2023



Informationssicherheitskonzept für den Landkreis Lüchow-Dannenberg

Versionierung

Version	Datum	Freigegeben durch	Änderungen
1.0	18.11.2022	Landrätin, IS-Team, FD 10	
2.0	29.09.2023	DSB, ISB	Erfassung weiterer IT-Grundschutz-Bausteine und Anpassungen an die Version 2023 der IT-Grundschutz-Bausteine
	11.10.2023	FD 10 FG Organisation	
	18.10.2023	FDL 16	
	30.10.2023	FDL 10	
	02.11.2023	PR	
	06.11.2023	Landrätin	

Inhalt

1. Einleitung

Die Erarbeitung des Informationssicherheitskonzepts (IS-Konzept) erfolgte auf Basis des IT-Grundschutzes des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Es wird die BSI-Standard-Absicherung umgesetzt.

2. Ziele des Informationssicherheitskonzepts

Ziel und Zweck des Konzepts ist die Einhaltung der drei primären, in der Informationssicherheitsleitlinie benannten Sicherheitsziele der Kreisverwaltung:

- Vertraulichkeit = Die Information ist lediglich für autorisierte Personen und Prozesse zugänglich.
- Verfügbarkeit = Die Information ist für die berechtigte Nutzerin oder den berechtigten Nutzer verfügbar und nutzbar.
- Integrität = Die Information ist richtig und vollständig. Veränderungen werden erkannt.

3. Geltungsbereich

Das Informationssicherheitskonzept gilt für alle Mitarbeitenden des Landkreises Lüchow-Dannenberg.

4. Verantwortlichkeiten/Zuständigkeiten

Die Ansprechperson zu allen Fragen dieses Konzepts ist die Informationssicherheitsbeauftragte oder der Informationssicherheitsbeauftragte (ISB).

Das Informationssicherheitskonzept wurde von der Verwaltungsleitung freigegeben. Der Verwaltungsleitung obliegt die Verantwortung für die Informationssicherheit des Landkreises Lüchow-Dannenberg. Sie verabschiedet auf Vorschlag der ISB oder des ISB dieses Informationssicherheitskonzept.

Alle Mitarbeitenden haben in ihren Aufgabenbereichen dafür zu sorgen, dass die Regelungen dieses Informationssicherheitskonzepts eingehalten werden. Zusätzlich haben die Führungskräfte ebenfalls auf die Einhaltung der Informationssicherheitsregelungen in ihren Organisationseinheiten zu achten.

5. Prozessorientierte Bausteine

HINWEIS: Detaillierte Beschreibungen zu den elementaren Gefährdungen finden sich im IT-Grundschutz-Kompendium des BSI.

ISMS = Managementsysteme für Informationssicherheit
ORP = Organisation und Personal
CON = Konzepte und Vorgehensweisen
OPS = Betrieb
DER = Detektion und Reaktion

ISMS.1 Sicherheitsmanagement	
Beschreibung	Das Informationssicherheitsmanagement dient der Herstellung und Optimierung von Informationssicherheit.
Anforderungen	
ISMS.1.A.1 Übernahme der Gesamtverantwortung	• Freigabe der ISLL und des IS-Konzepts

für Informationssicherheit durch die Verwaltungsleitung	• Mitglied im Informationssicherheitsteam (IS-Team) • Regelmäßige Managementberichte durch ISB an VL
ISMS.1.A.2 Festlegung der Sicherheitsziele und -strategie	• Sicherheitsziele und –strategie werden in der ISLL und dem IS-Konzept dokumentiert. • Die Überprüfung erfolgt jährlich.
ISMS.1.A3 Erstellung einer Leitlinie zur Informationssicherheit (ISLL)	• Die ISLL ist erstellt und wird jährlich überprüft. • Die ISLL wird über das Dokumentenmanagementsystem (DMS) allen Mitarbeitenden bekannt gegeben.
ISMS.1.A4 Benennung eines Informationssicherheitsbeauftragten	• Die ISB ist in Person von Frau Sabrina Donner benannt.
ISMS.1.A6 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit	• Das IS-Team setzt sich zusammen aus der VL, der Datenschutzbeauftragten oder dem Datenschutzbeauftragten, der FDL 16, der ISB oder dem ISB und Mitgliedern des Personalrats. • Das IS-Team trifft sich regelmäßig.
ISMS.1.A7 Festlegung von Sicherheitsmaßnahmen	• Die Sicherheitsmaßnahmen sind entsprechend des IT-Grundschutz-Kompendiums beschrieben und festgelegt. • Die Sicherheitsmaßnahmen werden regelmäßig überprüft.
ISMS.1.A8 Integration der Mitarbeitenden in den Sicherheitsprozess	• Den Mitarbeitenden sind die ISLL und das IS-Konzept bekannt gegeben und stehen im DMS jederzeit zur Verfügung. • Es erfolgen regelmäßig Schulungen zur Sensibilisierung.
ISMS.1.A9 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse	• Die ISB oder der ISB wird bei sicherheitsrelevanten Entscheidungen frühzeitig beteiligt.
ISMS.1.A10 Erstellung eines Sicherheitskonzepts	• Das Sicherheitskonzept ist erstellt und wird jährlich überprüft.
ISMS.1.A11 Aufrechterhaltung der Informationssicherheit	• Alle Dokumente zur IS werden jährlich (oder bei rechtlichen, organisatorischen Änderungen) geprüft und angepasst. • Sicherheitsrevisionen werden regelmäßig durchgeführt und dokumentiert. • Korrekturmaßnahmen zur Mängelbeseitigung werden durchgeführt.
ISMS.1.A12 Management-Berichte zur Informationssicherheit	• Quartalsweise erfolgen Managementberichte durch die ISB oder den ISB an die VL. Diese werden über das DMS revisionssicher archiviert. • Managemententscheidungen werden dokumentiert und revisionssicher über das DMS archiviert.
ISMS.1.A13 Dokumentation des Sicherheitsprozesses	• Der Ablauf des Sicherheitsprozesses wird dokumentiert. • Über das DMS stehen die aktuellsten Versionen der IS-Dokumente entsprechend der Berechtigungen im DMS zur Verfügung. Die Archivierung erfolgt ebenfalls revisionssicher über das DMS.
ISMS.1.A15 Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit	• Für festgelegte Sicherheitsmaßnahmen werden die erforderlichen Ressourcen geplant und termingerecht zur Verfügung gestellt.

ORP.1 Organisation	
Beschreibung	Der Baustein bildet die übergeordnete Basis, um Informationssicherheit in einer Institution umzusetzen. Anforderungen im Bereich der Organisation tragen dazu bei, das Niveau der Informationssicherheit zu erhöhen und zu erhalten.
Anforderungen	
ORP.1.A1 Festlegung von Verantwortlichkeiten und Regelungen	• Aufgaben, Funktionen, Organisationsstrukturen sind durch das Organigramm, die Organisationspläne und die Verwaltungsgliederungspläne eindeutig geregelt. Die IS-Leitlinie und das IS-Konzept gelten für alle Mitarbeitenden des Landkreises Lüchow-Dannenberg. Änderungen werden den Mitarbeitenden des Landkreises Lüchow-Dannenberg bekannt gegeben.
ORP.1.A2 Zuweisung der Zuständigkeiten	• Im Rahmen der Strukturanalyse sind die Zuständigkeiten dokumentiert und bekannt.
ORP.1.A3 Beaufsichtigung oder Begleitung von Fremdpersonen	• Institutionsfremde Personen melden sich in der Telefonzentrale im Foyer an. Die Mitarbeitenden werden durch die Mitarbeiterin bzw. den Mitarbeiter der Telefonzentrale über das Eintreffen der Besucherin bzw. des Besuchers informiert. Im Anschluss wird der Besucherin bzw. dem Besucher durch die Telefonzentrale das entsprechende Stockwerk mitgeteilt, zu welchem sie bzw. er sich eigenständig begeben kann. • Im Treppenhaus sind pro Etage Wartebereiche eingerichtet und entsprechend gekennzeichnet. Die jeweilige Mitarbeiterin bzw. der jeweilige Mitarbeiter holt die Besucherin bzw. den Besucher aus dem Wartebereich ab und begleitet diese bzw. diesen auch dorthin zurück. • Die Büroflure hinter den Glastüren dürfen nur in Begleitung einer bzw. eines Mitarbeitenden betreten werden. An den entsprechenden Glastüren werden dazu Hinweisschilder angebracht. • Im Treppenhaus können sich die institutionsfremden Personen frei bewegen, um sich ggf. Ausstellungen anzusehen oder die Toilettenräume aufzusuchen. Außerhalb des Treppenhauses sollen sich keine institutsfremden Personen unbeaufsichtigt aufhalten. Die Mitarbeitenden werden angehalten, institutionsfremde Personen ohne Begleitung auf den Bürofluren anzusprechen. • Weiterhin gilt, dass institutionsfremde Personen in allen Räumen des Landkreises Lüchow-Dannenberg beaufsichtigt werden sollen. Darüber hinaus ist darauf zu achten, dass keine institutsfremden Personen über die Nebeneingänge Zugang zum Kreishaus erhalten. • Folgende Personengruppen gelten nicht als institutsfremd: ➢ Mitglieder der politischen Gremien ➢ Mitarbeitende der LSE ➢ Mitglieder des Kats-Stabs ➢ Bürgermeisterinnen und Bürgermeister der

	Samtgemeinden und kreiseigenen Gemeinden ➢ Mitarbeitende der Bundeswehr ➢ Mitarbeitende der Polizei ➢ Mitarbeitenden des Rettungsdienstes ➢ Mitarbeitende der Feuerwehr
ORP.1.A4 Funktionstrennung zwischen unvereinbaren Aufgaben	• Operative und kontrollierende Aufgaben sind auf verschiedene Personen verteilt, z.B. RPA, ISB.
ORP.1.A15 Ansprechperson zu Informationssicherheitsfragen	• Ansprechperson zu Informationssicherheitsfragen sind bei dem Landkreis Lüchow-Dannenberg ISB und FDL 16.
ORP.1.A8 Betriebsmittel- und Geräteverwaltung	• Die Hardware ist inventarisiert und in ausreichender Menge vorhanden. Die Bereitstellung erfolgt über einen Berechtigungsantrag, welcher von der Fachdienst-/Stabstellenleitung, der DSB oder dem DSB, der FD 16 und dem Fachdienst 20 genehmigt werden muss. • Für die Entsorgung liegen ein Zertifikat von der Deutschen Aktenvernichtungsgesellschaft und ein Zertifikat von der Integra Dannenberg vor.
ORP.1.A13 Sicherheit bei Umzügen	• Für interne und externe Umzüge gibt die „Sicherheitsrichtlinie für Umzüge des Landkreises Lüchow-Dannenberg“
ORP.1.A16 Richtlinie zur sicheren IT-Nutzung	• Neue Mitarbeitende unterschreiben bei der Einstellung die Erklärung für die Nutzung von elektronischen Kommunikationsmitteln bei der Kreisverwaltung Lüchow-Dannenberg im Sinne der dazu ergangenen Dienstanweisung

ORP.2 Personal	
Beschreibung	Die Mitarbeitenden haben die Aufgabe, Informationssicherheit umzusetzen.
Anforderungen	
ORP.2.A1 Geregelte Einarbeitung neuer Mitarbeitenden	• Die erste Einführung erfolgt durch die FG Personal des FD 10. • Dort erhält der Mitarbeitende ebenfalls Informationen zur AGA, zur Schweigepflicht und dem Datenschutz, die FAQ des FD 16, einen Personalfragebogen und das Willkommensheft. • Neue Mitarbeitende führt die Vorgesetzte oder der Vorgesetzte in das Aufgabengebiet ein; dabei bedient sie oder er sich der Hilfe von erfahrenen Mitarbeitenden.
ORP.2.A2 Geregelte Verfahrensweise beim Weggang von Mitarbeitenden	• Entsprechend der Schweigepflichtserklärung ist die Schweigepflicht auch nach Ausscheiden einzuhalten. • Ausscheidende Mitarbeitende geben alle Schlüssel, Geräte, Ausweise und ggf. weitere Unterlagen zurück. • Die FG Personal meldet das Ausscheiden an den FD 16 zur digitalen Deaktivierung und Löschung. • Der Weggang von Mitarbeitenden wird von der FG Personal begleitet.
ORP.2.A3 Festlegung von Vertretungsregelungen	• Vertretungsregelungen sind in dem Geschäftsverteilungsplan erfasst.
ORP.2.A4 Festlegung von Regelungen für den Einsatz von Fremdpersonal	• Es erfolgt der Einsatz von Fremdpersonal im Rahmen des Katastrophenschutzstabs.
ORP.2.A5 Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal	• Regelungen zur Informationssicherheit für Mitglieder des Katastrophenschutzstabs sind erfolgt und müssen von externen Mitgliedern des Katastrophenschutzstabs unterschrieben

	werden.
ORP.2.A14 Aufgaben und Zuständigkeiten von Mitarbeitenden	• Die Aufgaben und Zuständigkeiten sind im Geschäftsverteilungsplan geregelt.
ORP.2.A15 Qualifikation des Personals	• Die Mitarbeitenden haben die Pflicht, ihre dienstlichen Kenntnisse regelmäßig durch Teilnahme an Fortbildungsveranstaltungen weiterzuentwickeln.
ORP.2.A7 Überprüfung der Vertrauenswürdigkeit von Mitarbeitenden	• Im Rahmen der Einstellung erfolgt die Prüfung der Vertrauenswürdigkeit.

ORP.3 Sensibilisierung und Schulung zur Informationssicherheit	
Beschreibung	Die Mitarbeitenden haben ein Sicherheitsbewusstsein und sind für Gefährdungen sensibilisiert. Ihre Verantwortung im Rahmen der Informationssicherheit ist Ihnen bekannt.
Anforderungen	
ORP.3.A1 Sensibilisierung der Institutionsleitung für Informationssicherheit	• Die Verwaltungsleitung ist Teil des IS-Teams und fördert die Schulungsmaßnahmen. • Die Führungskräfte haben ebenfalls auf die Einhaltung der Informationssicherheitsregelungen in ihren Organisationseinheiten zu achten.
ORP.3.A3 Einweisung des Personals in den sicheren Umgang mit IT	• Die Einweisung erfolgt innerhalb der Fachdienste. • Die Erklärung zur Nutzung der IT-Geräte bestimmt die Nutzung und den Einsatz der IT-Geräte. Die Erklärung muss von allen neuen Mitarbeitenden unterzeichnet werden.
ORP.3.A4 Konzeption und Planung eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit	• Die Sensibilisierung und Schulung findet im Rahmen einer Präsentation statt und wird entsprechend der ISLL und des IS-Konzepts aktualisiert.
ORP.3.A6 Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit	• Alle Mitarbeitenden werden jährlich durch eine Schulung sensibilisiert.
ORP.3.A7 Schulung zur Vorgehensweise nach IT-Grundschutz	• Die ISB oder der ISB ist mit dem IT-Grundschutz vertraut. • Die ISB oder der ISB ist zertifiziert.
ORP.3.A8 Messung und Auswertung des Lernerfolgs	• Die Messung und Auswertung der Lernerfolge erfolgt anonymisiert über eine Awareness Software

ORP.4 Identitäts- und Berechtigungsmanagement	
Beschreibung	Der Zugang zu Informationen erfolgt über die Berechtigungen einer oder eines Benutzenden.
Anforderungen	
ORP.4.A1 Regelung für die Einrichtung und Löschung von Benutzenden und Benutzendengruppen	• Benutzende sowie Benutzendengruppen werden ausschließlich von dem FD 16 oder den Softwareadministratorinnen oder Softwareadministratoren (für Fachanwendungen) eingerichtet und deaktiviert bzw. gelöscht. • Allen Benutzenden ist eine eindeutige Benutzendenerkennung zugeordnet.
ORP.4.A2 Einrichtung, Änderung und Entzug von Berechtigungen	• Berechtigungen erfolgen entsprechend des tatsächlichen Bedarfs über einen Berechtigungsantrag, welcher von der Fachdienst-/Stabstellenleitung, der DSB oder dem DSB, dem FD 16 und FD20 genehmigt werden muss. • Bei Ausscheiden/Wechsel von Mitarbeitenden werden die Berechtigungen von dem FD 16, nach Mitteilung durch die FG Personal des FD

	10, entzogen.
ORP.4.A3 Dokumentation der Benutzendenkennungen und Rechteprofile	• Die Berechtigungsvergabe erfolgt Workflow gesteuert und wird programmgestützt dokumentiert. Der Zugriff auf die Dokumentation ist nur den berechtigten Personen möglich.
ORP.4.A4 Aufgabenverteilung und Funktionstrennung	• Es gibt keine definierten unvereinbaren Aufgaben und Funktionen.
ORP.4.A5 Vergabe von Zutrittsberechtigungen	• Die Vergabe und Dokumentation der Schlüssel erfolgt durch das Gebäudemanagement. Die Vergabe und Dokumentation der Zeiterfassungschips, welche auch den Zutritt über den Personaleingang in das Kreishaus gewährleisten, erfolgt durch den Fachdienst 10.
ORP.4.A6 Vergabe von Zugangsberechtigungen	• Die Vergabe und Dokumentation der Zeiterfassungschips, welche zur Nutzung der Multifunktionsgeräte benötigt werden, erfolgt durch den Fachdienst 10. Die Schlüsselvergabe und Dokumentation zum Öffnen der Räume erfolgt pro Mitarbeitenden entsprechend ihrer oder seiner Zugangsberechtigung durch das Gebäudemanagement.
ORP.4.A7 Vergabe von Zugriffsrechten	• Die Vergabe und Dokumentation der Zugriffsrechte erfolgt entsprechend der Funktion, welche durch den Fachdienst 10 festgelegt ist.
ORP.4.A8 Regelung des Passwortgebrauchs	• Derzeit genügt die alleinige Authentisierung mit dem Passwort des Benutzenden. Das Passwort unterliegt Richtlinien, worin eine Mindestsicherheitsanforderung definiert ist. Die mehrfache Verwendung von Passwörtern kann technisch nicht ausgeschlossen werden, da diverse Anwendungen keine Anbindung vom Fachverfahren zum Windows Verzeichnisdienst haben. • Mind. acht Zeichen • Groß- und Kleinschreibung, Sonderzeichen, Ziffern • Das vollständige Passwort sollte **nicht** in Wörterbüchern vorkommen. • Es sollte **nicht** aus Wiederholungs- oder Tastaturmustern bestehen, wie z.B. „asdfg“ oder „1234abcd“. • Ziffern oder Sonderzeichen am Anfang oder Ende eines ansonsten simplen Passworts sind nicht sicher. • Voreingestellte Passwörter **immer** ändern! • **Keine** Passwörter per E-Mail verschicken! • Passwörter sind nicht mehrfach zu verwenden. • Passwörter müssen geheim gehalten werden, dürfen nur unbeobachtet eingegeben werden und müssen gewechselt werden, wenn es unautorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht. • Bei einer schriftlichen Hinterlegung für den Notfall, ist das Passwort sicher aufzubewahren, also bspw. nicht unter der Tastatur, dem Monitor, der Kaffee-/Teetasse.
ORP.4.A9 Identifikation und Authentisierung	• Für den Zugriff auf IT-Systeme und Dienste ist eine Identifikation und Authentisierung durch die Eingabe eines Benutzendennamens und Passworts erforderlich.
ORP.4.A22 Regelung zur Passwortqualität	• Die Qualität der Passwörter wird durch Richtlinien gewährleistet.
ORP.4.A23 Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme	• Da durch die verschiedenen Fachverfahren nicht gewährleistet werden kann, dass eine

	Kompromittierung erkannt wird, müssen Passwörter in regelmäßigen Abständen geändert werden. • Passwortwechsel für Dienstkonten etc. werden geplant und gemeinsam mit dem/der betroffenen Fachdienst/Stabstelle abgestimmt.
ORP.4.A11 Zurücksetzen von Passwörtern	• Passwörter werden grundsätzlich telefonisch zurückgesetzt. Das neue Passwort wird ebenfalls ausschließlich telefonisch dem/der Mitarbeitenden mitgeteilt.
ORP.4.A12 Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen	• Ein Authentisierungskonzept wird derzeit nicht benötigt, da für alle Systeme und Verfahren die Anmeldung durch Benutzendenname und Passwort erfolgt.
ORP.4.A13 Geeignete Auswahl von Authentisierungsmechanismen	• Eine Sperrung der oder des Benutzenden nach wiederholter Falscheingabe des Passwortes ist, soweit es das Fachverfahren ermöglich, eingerichtet.
ORP.4.A14 Kontrolle der Wirksamkeit der Benutzendentrennung am IT-System bzw. an der Anwendung	• Benutzende werden bei Inaktivität gesperrt.
ORP.4.A16 Richtlinien für die Zugriffs- und Zugangskontrolle	• Im zentralen Windows-Verzeichnisdienst sind diverse Gruppen für jegliche Fachdienste/Fachanwendungen und Berechtigungen definiert. Hierrüber wird auch ein Standard definiert.
ORP.4.A17 Geeignete Auswahl von Identitäts- und Berechtigungsmanagement-Systemen	• Es ist neben dem Windows-Verzeichnisdienst kein zusätzliches Identitäts- und Berechtigungsmanagement-System im Einsatz.
ORP.4.A18 Einsatz eines zentralen Authentisierungsdienstes	• Nicht im Einsatz.
ORP.4.A19 Einweisung aller Mitarbeitenden in den Umgang mit Authentisierungsverfahren und -mechanismen	• Nicht im Einsatz.

ORP.5 Compliance Management (Anforderungsmanagement)	
Beschreibung	Gesetzliche, vertragliche und sonstige Anforderungen müssen eingehalten werden.
Anforderungen	
ORP.5.A1 Identifikation der Rahmenbedingungen	• Die gesetzlichen, vertraglichen und sonstigen Vorgaben sind von der ISB oder dem ISB in einer Übersicht gelistet. Diese wird regelmäßig überprüft und ggf. angepasst.
ORP.5.A2 Beachtung der Rahmenbedingungen	• Die als sicherheitsrelevant identifizierten Anforderungen werden bei der Einführung von neuen Geschäftsprozessen, Anwendungen und IT-Systemen berücksichtigt. Bei Verstößen gegen die o.g. Anforderungen, werden Korrekturmaßnahmen ergriffen.
ORP.5.A4 Konzeption und Organisation des Compliance Managements	• Alle relevanten gesetzlichen, vertraglichen und sonstigen Vorgaben mit Auswirkungen auf das Informationssicherheitsmanagement werden von den Führungskräften identifiziert und mit der ISB oder dem ISB kommuniziert.
ORP.5.A5 Ausnahmegenehmigungen	• Ausnahmegenehmigungen werden derzeit nicht benötigt.
ORP.5.A8 Regelmäßige Überprüfungen des Compliance Managements	• Die Anforderungen und Maßnahmen werden regelmäßig von der ISB oder dem ISB geprüft. Diese findet in Zusammenarbeit mit den Führungskräften statt.

CON.1 Kryptokonzept	
Beschreibung	Mit Hilfe von kryptografischen Verfahren werden Informationen verschlüsselt, sodass deren Inhalt ohne den zugehörigen Schlüssel nicht lesbar ist.
Es werden keine kryptografischen Verfahren eingesetzt.	

CON.3 Datensicherungskonzept	
Beschreibung	Datenverluste sollen durch regelmäßige Datensicherungen minimiert werden.
Anforderungen	
CON.3.A1 Erhebung der Einflussfaktoren für Datensicherungen	• Die Rahmenbedingungen und Einflussfaktoren werden im Datensicherungskonzept benannt. • Das Konzept wird bei Veränderungen aktualisiert.
CON.3.A2 Festlegung der Verfahrensweisen für die Datensicherung	• Die Verfahrensweisen für die Datensicherung sind im Datensicherungskonzept beschrieben.
CON.3.A4 Erstellung von Datensicherungsplänen	• Die Vorgaben zur Datensicherung beinhaltet das Datensicherungskonzept.
CON.3.A5 Regelmäßige Datensicherung	• Die Mitarbeitenden des FD 16 sind über die Regelungen zur Datensicherung informiert. • Die Datensicherungen finden planmäßig statt.
CON.3.A12 Sichere Aufbewahrung der Speichermedien für die Datensicherungen	• Die Datensicherungen werden räumlich getrennt und in einem anderen Brandabschnitt aufbewahrt. • Die monatlichen und jährlichen Tapes werden in einem anderen Gebäude aufbewahrt.
CON.3.A14 Schutz von Datensicherungen	• Die Datensicherungen sind vor unbefugtem Zugriff geschützt. • Lediglich autorisierte Mitarbeitende des FD 16 können auf die Datensicherungen zugreifen.
CON.3.A15 Regelmäßiges Testen der Datensicherungen	• Die Datensicherungen werden regelmäßig durch den FD 16 getestet. Hierbei werden sowohl einzelne Dateien sowieso gesamte virtuelle Server von NAS oder Tape wiederhergestellt. Ebenso wird eine Rücksicherung von einzelnen Mails aus Exchange getestet.
CON.3.A6 Entwicklung eines Datensicherungskonzepts	• Das Datensicherungskonzept für den Landkreis Lüchow-Dannenberg ist erstellt.
CON.3.A7 Beschaffung eines geeigneten Datensicherungssystem	• Es existiert ein Datensicherungssystem.
CON.3.A9 Voraussetzungen für die Online-Datensicherung	• Es werden keine Online-Datensicherungen durchgeführt.

CON.6 Löschen und Vernichten	
Beschreibung	Datenträger (z.B. Papier, Filme, Festplatten, CDs etc.) sind sicher zu löschen bzw. zu vernichten.
Anforderungen	
CON.6.A1 Regelung für die Löschung und Vernichtung von Informationen	• Das Löschen und Vernichten von Informationen ist in den Fachdiensten und Stabstellen entsprechend der gesetzlichen Vorschriften geregelt.
CON.6.A2 Ordnungsgemäßes Löschen und Vernichten von schützenswerten Betriebsmitteln und Informationen	• Datenträger werden im abgesicherten Bereich in einem gesonderten Container aufbewahrt. Dieser verfügt über eine Fallklappe. Den Schlüssel zum Container hat ausschließlich die FDL 16.
CON.6.A11 Löschung und Vernichtung von Datenträgern durch externe Dienstleister	• Erfolgt durch die Deutsche Aktenvernichtung • DAV GmbH.
CON.6.A12 Mindestanforderungen an Verfahren	• Erfolgt durch die Deutsche Aktenvernichtung

zur Löschung und Vernichtung	• DAV GmbH.
CON.6.A4 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern	• Erfolgt durch die Deutsche Aktenvernichtung • DAV GmbH.
CON.6.A8 Erstellung einer Richtlinie für die Löschung und Vernichtung von Informationen	• Erfolgt durch die Deutsche Aktenvernichtung • DAV GmbH.
CON.6.A13 Vernichtung defekter digitaler Datenträger	• Erfolgt durch die Deutsche Aktenvernichtung • DAV GmbH.

CON.7 Informationssicherheit auf Auslandsreisen	
Beschreibung	Bei Dienstreisen, vor allem ins Ausland, gibt es eine Vielzahl an Bedrohungen und Risiken für die Informationssicherheit, die im normalen Geschäftsbetrieb nicht existieren. Jede Reise ist individuell zu bewerten, da sich aufgrund der Kombination aus Reisezweck (geschäftliche Besprechung, Tagung, Kongress etc.), Reisedauer und Reiseziel jeweils eine neue Bedrohungslage ergibt, auch in Bezug auf den Schutz geschäftskritischer Informationen. Die Bedrohungslage ist auf Reisen besonders erhöht.
In der Regel finden repräsentative Auslandsreisen ohne Mitnahme von kreiseigener Hardware oder sicherheitsrelevanten Daten statt. In Ausnahmefällen wird mit der oder dem Mitarbeitenden eine Einzelvereinbarung getroffen. Grundsätzlich gelten dann die Regelungen für das mobile Arbeiten.	

CON.8 Software-Entwicklung	
Beschreibung	Eigene Entwicklung von Software-Lösungen (Auftragnehmerseite).
Es wird keine eigene Software entwickelt.	

CON.9 Festlegung zulässiger Empfänger/innen	
Beschreibung	Informationen werden zwischen Senderin oder Sender und Empfängerin oder Empfänger über unterschiedliche Kommunikationswege übertragen, wie z B. persönliche Gespräche, Telefonate, Briefpost, Wechseldatenträger oder Datennetze. Regeln zum Informationsaustausch stellen sicher, dass vertrauliche Informationen nur an berechtigte Personen weitergegeben werden.
Anforderungen	
CON.9.A1 Festlegung zulässiger Empfängerinnen und Empfänger	• Die Einweisung und Festlegung erfolgt durch die DSB oder den ISB.
CON.9.A2 Regelung des Informationsaustausches	• Die Klassifizierung der Informationen ist erfolgt und den Mitarbeitenden bekannt gegeben.
CON.9.A3 Unterweisung des Personals zum Informationsaustausch	• Die DSB oder der DSB schult die Mitarbeitenden. • Schulungsunterlagen werden im DMS nscale hinterlegt.
CON.9.A4 Vereinbarungen zum Informationsaustausch mit Externen	• Zwischen allen Landes- und Bundesbehörden erfolgt die Verschlüsselung durch das Landesnetz. • Der Informationsaustausch mit dem Gericht erfolgt über das besondere elektronische Behördenpostfach (beBPo).
CON.9.A5 Beseitigung von Restinformationen vor Weitergabe	• Die Anhänge werden vor der Weiterleitung von E-Mails geprüft. • Es werden ausschließlich benötigte Daten oder Ausschnitte versandt.
CON.9.A6 Kompatibilitätsprüfung des Sender- und Empfängersystems	• Die Kompatibilität ist sichergestellt.
CON.9.A7 Sicherungskopie der übermittelten Daten	• Bei der Übermittlung von Originaldateien verbleiben Kopien bei der Absenderin oder dem Absender. • Digitale Dateien werden im DMS nscale revisionssicher abgelegt.

CON.9.A8 Verschlüsselung und digitale Signatur	• Die Verschlüsselung ist sichergestellt (Landesnetz & KDO-KomBox).

CON.10 Entwicklung von Webanwendungen	
Beschreibung	Entwicklung sicherer Webanwendungen und Schutz von Informationen, die durch diese Webanwendungen verarbeitet werden.
Es werden keine Webanwendungen entwickelt.	

OPS.1.1.1 Allgemeiner IT-Betrieb	
Beschreibung	Der IT-Betrieb stellt eine Organisationseinheit und den zugehörigen Geschäftsprozess innerhalb der Informationstechnik dar. Der Prozess beschreibt die Aufgaben mit allen Tätigkeiten, die durch die Organisationseinheit IT-Betrieb umgesetzt werden. Die IT umfasst alle IT-Komponenten einer Institution, insbesondere IT-Systeme, -Dienste, -Anwendungen, -Plattformen und Netze.
Anforderungen	
OPS.1.1.1.A1 Festlegung der Aufgaben und Zuständigkeiten des IT-Betriebs	• Die Aufgaben und Rechte sind im FD 16 geregelt. Meldewege und Schnittstellen sind bekannt.
OPS.1.1.1.A3 Erstellen von Betriebshandbüchern für die betriebene IT	• Betriebshandbücher liegen vor. Nach Bedarf werden neue Betriebshandbücher erstellt bzw. bestehende aktualisiert.
OPS.1.1.1.A4 Bereitstellen ausreichender Personal- und Sachressourcen	• Derzeit stehen keine ausreichenden Personalressourcen zur Verfügung. • Benötigte Sachressourcen sind vorhanden. Neuanschaffungen werden bei der Haushaltsplanung berücksichtigt.
OPS.1.1.1.A6 Durchführung des IT-Asset-Managements	• Die IT-Assets werden in INDART gepflegt.
OPS.1.1.1.A13 Absicherung der Betriebsmittel und der Dokumentation	• Auf die Betriebsmittel, Dokumentationen und Handbücher können ausschließlich die berechtigten Personen des FD 16 zugreifen.
OPS.1.1.1.A14 Berücksichtigung der Betreibbarkeit bei Konzeption und Beschaffung	• Bei der Konzeption und Beschaffung von IT-Komponenten werden Anforderungen für einen effizienten und sicheren Betrieb berücksichtigt.
OPS.1.1.1.A15 Planung und Einsatz von Betriebsmitteln	• Der FD 16 plant, beschafft und setzt für alle IT-Komponenten die Betriebsmittel bedarfsgerecht ein. • Anforderungen an die jeweiligen Betriebsmittel werden mit den anderen betroffenen Organisationseinheiten abgestimmt.
OPS.1.1.1.A16 Schulung des Betriebspersonals	• Für das Personal des FD 16 steht jährlich ein Budget für Fortbildungen zur Verfügung. • Fortbildungen können von jedem Mitarbeitenden nach Bedarf beantragt und besucht werden.
OPS.1.1.1.A17 Planung des IT-Betriebs unter besonderer Berücksichtigung von Mangel- und Notsituationen	• Eine Priorisierung der IT-Komponenten findet im Rahmen der Notfallplanung statt. • Das Notfallmanagement beinhaltet u.a. Wiederanlaufpläne und ein Notfallhandbuch für die IT-Komponenten.
OPS.1.1.1.A18 Planung des Einsatzes von Dienstleistenden	• Der Einsatz von Dienstleistenden wird vom FD 16 koordiniert. • In der Fachgruppe gibt es für den Dienstleistenden eine Ansprechperson.
OPS.1.1.1.A19 Regelungen für Wartungs- und Reparaturarbeiten	• Die IT-Komponenten werden regelmäßig gewartet. • Eine Ansprechperson für die jeweilige IT-Komponente ist benannt. • Wartungs-oder Reparaturarbeiten durch Dienstleistende werden von der Ansprechperson autorisiert, begleitet bzw. unterstützt.

OPS.1.1.1.A20 Prüfen auf Schwachstellen	• Der FD 16 informiert sich regelmäßig über bekannt gewordene Schwachstellen. • Schwachstellen werden schnellstmöglich behoben. • Solange keine entsprechenden • Patches zur Verfügung stehen, werden für schwerwiegende Schwachstellen und Bedrohungen andere Maßnahmen zum Schutz der IT-Komponente getroffen. Falls dies für eine IT-Komponente nicht möglich ist, wird geprüft, ob diese noch weiter betrieben werden kann.

OPS.1.1.2 Ordnungsgemäße IT-Administration	
Beschreibung	Einsatz einer ordnungsgemäßen IT-Administration, mit der die Sicherheitsanforderungen von IT-Anwendungen, -Systemen und Netzen erfüllt werden
Anforderungen	
OPS.1.1.2.A2 Vertretungsregelungen und Notfallvorsorge	• Die Zugänge zu allen zu betreuenden IT-Systemen sind dokumentiert und liegen den Vertreterinnen oder den Vertretern im Notfall vor.
OPS.1.1.2.A4 Beendigung der Tätigkeit als IT-Administratorin oder IT-Administrator	• Wenn eine Administratorin oder ein Administrator den Landkreis Lüchow-Dannenberg verlässt, wird der Benutzende und alle ihre oder seine Zugänge unmittelbar deaktiviert. Weitere bekannte Passwörter werden ebenfalls geändert.
OPS.1.1.2.A5 Nachweisbarkeit von administrativen Tätigkeiten	• Generell verfügt jede Administratorin und jeder Administrator über eine eigene Benutzendenkennung im Netzwerk.
OPS.1.1.2.A7 Regelung der IT-Administrationstätigkeit	• Die IT-Administrationstätigkeiten sind in der „Richtlinie zur Regelung der IT-Administrationstätigkeit für den Landkreis Lüchow-Dannenberg“ geregelt.
OPS.1.1.2.A8 Administration von Fachanwendungen	• Die Administration von Fachanwendungen ist in der „Richtlinie zur Regelung der IT-Administrationstätigkeit für den Landkreis Lüchow-Dannenberg“ geregelt.
OPS.1.1.2.A11 Dokumentation von IT-Administrationstätigkeiten	• Systemänderungen durch die IT-Administration werden in einer Excel-Tabelle dokumentiert.

OPS.1.1.3 Patch- und Änderungsmanagement	
Beschreibung	Aufbau eines Patchmanagements inkl. Kontrolle und Optimierung, sowie die Kernaspekte zur Informationssicherheit eines Änderungsmanagements.
Anforderungen	
OPS.1.1.3.A1 Konzept für das Patch- und Änderungsmanagement	• Ein Konzept für das Patch- und Änderungsmanagement liegt vor.
OPS.1.1.3.A2 Festlegung der Zuständigkeiten	• Zuständig für die technische Umsetzung sind die Mitarbeitenden des FD 16. • Fachlich zuständig sind in den Organisationeinheiten die Fachadministratorin oder der Fachadministrator (wenn vorhanden) und die Leitung.
OPS.1.1.3.A3 Konfiguration von Autoupdate-Mechanismen	• Es werden keine Autoupdate-Mechanismen eingesetzt.
OPS.1.1.3.A15 Regelmäßige Aktualisierung von IT-Systemen und Software	• IT-Systeme und Software werden regelmäßig aktualisiert. • Patches werden zeitnah eingespielt. • Wird ein Patch nicht eingespielt, werden die Gründe dafür dokumentiert.

	• Wenn Hardware- oder Software-Produkte eingesetzt werden, die nicht mehr von den Herstellenden unterstützt werden oder für die kein Support mehr vorhanden ist, wird geprüft ob diese dennoch sicher betrieben werden können. Ist dies nicht der Fall, werden diese Hardware- oder Software-Produkte nicht mehr verwendet.
OPS.1.1.3.A5 Umgang mit Änderungsanforderungen	• Gewünschte/geplante Änderungen werden von der betroffenen OE mit dem FD 16 und der oder dem Mitarbeitenden für Softwareoptimierung besprochen. • Bei Änderungen, die die Informationssicherheit betreffen, ist die ISB oder der ISB zu beteiligen. Die ISB oder der ISB erteilt eine schriftliche Freigabe.
OPS.1.1.3.A6 Abstimmung von Änderungsanforderungen	• Gewünschte/geplante Änderungen werden von der betroffenen OE mit dem FD 16 und der oder dem Mitarbeitenden für Softwareoptimierung besprochen. • Bei Änderungen, die die Informationssicherheit betreffen, ist die ISB oder der ISB zu beteiligen. Die Informationssicherheitsbeauftragte erteilt eine schriftliche Freigabe.
OPS.1.1.3.A7 Integration des Änderungsmanagements in die Geschäftsprozesse	• Änderungen werden in die betroffenen Geschäftsprozesse integriert. • Die betroffene OE berät sich hierzu mit der oder dem Mitarbeitenden für Prozessoptimierung. • Erfolgen die Änderungen seitens des FD 16, werden alle betroffenen OE informiert.
OPS.1.1.3.A8 Sicherer Einsatz von Werkzeugen für das Patch- und Änderungsmanagement	• Einsatz des SCCM (System Center Configuration Manager) = Verteilung diverser Software • Updates für bestimmte Fachverfahren werden zum Teil direkt am Server eingespielt und dann durch das Fachverfahren an die PCs der Mitarbeitenden verteilt.
OPS.1.1.3.A9 Test- und Abnahmeverfahren für neue Hardware	• Bei der Auswahl neuer Hardware wird berücksichtigt, ob die eingesetzte Software und insbesondere die relevanten Betriebssysteme mit der Hardware und dessen Treibersoftware kompatibel sind. Der Einsatz neuer Hard- und Software wird vor Einführung getestet.
OPS.1.1.3.A10 Sicherstellung der Integrität und Authentizität von Softwarepaketen	• Die Authentizität und Integrität von Softwarepaketen wird geprüft und sichergestellt.
OPS.1.1.3.A11 Kontinuierliche Dokumentation der Informationsverarbeitung	• Änderungen werden im Rahmen von Vermerken dokumentiert.

OPS.1.1.4 Schutz vor Schadprogrammen	
Beschreibung	Effektiver Schutz gegen Schadprogramme. Schadprogramme sind Programme, die in der Regel ohne Wissen und Einwilligung des Benutzenden schädliche Funktionen auf einem IT-System ausführen. Schadprogramme können grundsätzlich auf allen Betriebssystemen und IT-Systemen ausgeführt werden. In diesem Baustein wird der Begriff „Virenschutzprogramm" verwendet. „Viren" stehen dabei als Synonym für alle Arten von Schadprogrammen. Gemeint ist mit „Virenschutzprogramm" demnach ein Programm zum Schutz vor jeglicher Art von Schadprogrammen.
Anforderungen	
OPS.1.1.4.A1 Erstellung eines Konzepts für den Schutz vor Schadprogrammen	• „Konzept für den Schutz vor Schadprogrammen für den Landkreis Lüchow-Dannenberg" ist entwickelt.
OPS.1.1.4.A2 Nutzung systemspezifischer	• Generell werden alle Standard-

Schutzmechanismen	Schutzmechanismen der IT-Systeme verwendet.
OPS.1.1.4.A3 Auswahl eines Virenschutzprogrammes	• Es wird ein Virenschutzprogramm eingesetzt, welches für den Enterprise-Bereich zugeschnitten ist.
OPS.1.1.4.A5 Betrieb und Konfiguration von Virenschutzprogrammen	• Es werden keine Funktionen auf Grund von Leistungsfähigkeit deaktiviert. Das Programm wird vollwertig mit allen Funktionen genutzt.
OPS.1.1.4.A6 Regelmäßige Aktualisierung der eingesetzten Virenschutzprogramme und Signaturen	• Das Virenschutzprogramm wird regelmäßig und dauerhaft aktualisiert. Die aktuellen Datenbanken werden regelmäßig auf die Clients verteilt.
OPS.1.1.4.A7 Sensibilisierung und Verpflichtung der Benutzenden	• Eine Sensibilisierung erfolgt über regelmäßige Mails, IS-Schulungen und die zur Verfügungsstellung des BITS (Behörden-IT-Sicherheitstraining).
OPS.1.1.4.A9 Meldung von Infektionen mit Schadprogrammen	• Das Virenschutzprogramm ist so definiert, dass eine Infektion sofort isoliert und an den Service-Desk gemeldet wird. Ein betroffener Arbeitsplatzrechner wird dann unmittelbar vom Netzwerk getrennt und Offline geprüft.

OPS.1.1.6 Software-Tests und -Freigaben	
Beschreibung	Dieser Baustein beschreibt den Test- und Freigabeprozess für jegliche Art von Software. Der Test- und Freigabeprozess zeichnet sich dadurch aus, dass dieser je nach Ergebnis mehrmals durchlaufen werden kann.
Anforderungen	
OPS.1.1.6.A1 Planung der Software-Tests	• Die Tests werden von der entsprechenden Organisationseinheit zusammen mit dem FD 16 und der ISB oder dem ISB geplant und durchgeführt.
OPS.1.1.6.A2 Durchführung von funktionalen Software-Tests	• Anwenderinnen und Anwender testen die Software zusammen mit dem FD 16 und der ISB oder dem ISB ohne den Produktivbetrieb zu beeinflussen.
OPS.1.1.6.A3 Auswertung der Testergebnisse	• Die Testergebnisse werden ausgewertet und dokumentiert.
OPS.1.1.6.A4 Freigabe der Software	• Die Freigabe der Software erfolgt schriftlich durch die zuständige Organisationseinheit. Darüber hinaus müssen die ISB oder der ISB und der FD 16 dem Einsatz der Software zustimmen.
OPS.1.1.6.A5 Durchführung von Software-Tests für nicht funktionale Anforderungen	• Die Tests werden von der entsprechenden Organisationseinheit zusammen mit dem FD 16 und der ISB oder dem ISB geplant und durchgeführt.
OPS.1.1.6.A11 Verwendung von anonymisierten oder pseudonymisierten Testdaten	• Die Tests erfolgen in Übungsdatenbanken mit fiktiven Fällen.
OPS.1.1.6.A6 Geordnete Einweisung der Software-Testenden	• Die Software-Testenden werden durch ihre Führungskraft oder ihre Fachadministration eingewiesen.
OPS.1.1.6.A7 Personalauswahl der Software-Testenden	• Die Software-Testenden werden von der zuständigen Organisationseinheit ausgewählt.
OPS.1.1.6.A10 Erstellung eines Abnahmeplans	• Die Tests und Freigaben werden dokumentiert. Die Ablehnung einer Freigabe muss schriftlich begründet werden.
OPS.1.1.6.A12 Durchführung von Regressionstests	• Regressionstests nach Updates werden durchgeführt und dokumentiert.
OPS.1.1.6.A13 Trennung der Testumgebung von der Produktivumgebung	• Für die Tests werden Testumgebungen (Übungsdatenbanken) genutzt.
OPS.1.1.6.A15 Überprüfung der Installation und zugehöriger Dokumentation	• Die Installation der Software erfolgt entsprechend deren Regelungen.

OPS.1.2.2 Archivierung	
Beschreibung	Die Archivierung spielt im Dokumentenmanagementprozess eine besondere Rolle. Denn es wird einerseits erwartet, dass die digitalen Dokumente bis zum Ablauf einer vorgegebenen Aufbewahrungsfrist verfügbar sind. Andererseits soll ihre Vertraulichkeit und Integrität bewahrt bleiben.
Anforderungen	
OPS.1.2.2.A1 Ermittlung von Einflussfaktoren für die elektronische Archivierung	• Die technischen, rechtlichen und organisatorischen Einflussfaktoren sind ermittelt und dokumentiert.
OPS.1.2.2.A3 Geeignete Aufstellung von Archivsystemen und Lagerung von Archivmedien	• Die IT-Komponenten befinden sich im gesicherten Bereich des FD 16.
OPS.1.2.2.A4 Konsistente Indizierung von Daten bei der Archivierung	• Struktur und Umfang der Indexangaben werden im Archivierungskonzept festgelegt.
OPS.1.2.2.A5 Regelmäßige Aufbereitung von archivierten Datenbeständen	• Die regelmäßige Aufbereitung von archivierten Datenbeständen ist möglich.
OPS.1.2.2.A6 Schutz der Integrität der Indexdatenbank von Archivsystemen	• Die Integrität der Daten ist sichergestellt.
OPS.1.2.2.A7 Regelmäßige Datensicherung der System- und Archivdaten	• Die Datensicherung erfolgt regelmäßig.
OPS.1.2.2.A8 Protokollierung der Archivzugriffe	• Alle Zugriffe auf die elektronischen Archive werden protokolliert,
OPS.1.2.2.A9 Auswahl geeigneter Datenformate für die Archivierung von Dokumenten	• Die Dokumente werden im PDF/A-Format archiviert.
OPS.1.2.2.A12 Überwachung der Speicherressourcen von Archivmedien	• Die Speicherressourcen werden überwacht.
OPS.1.2.2.A14 Regelmäßige Beobachtung des Marktes für Archivsysteme	• Der Markt für Archivsysteme wird regelmäßig beobachtet.
OPS.1.2.2.A15 Regelmäßige Aufbereitung von kryptografisch gesicherten Daten bei der Archivierung [IT-Betrieb]	• Es wird kein kryptografisches Verfahren eingesetzt.
OPS.1.2.2.A16 Regelmäßige Erneuerung technischer Archivsystem-Komponenten	• Neue Hard- und Software und Veränderungen werden geprüft und getestet.
OPS.1.2.2.A17 Auswahl eines geeigneten Archivsystems	• Ein geeignetes Archivsystem ist ausgewählt.
OPS.1.2.2.A18 Verwendung geeigneter Archivmedien	• Für die Archivierung geeignete Medien sind ausgewählt.

OPS.1.2.4 Telearbeit	
Beschreibung	Unter Telearbeit wird jede auf die Informations- und Kommunikationstechnik gestützte Tätigkeit verstanden, die ganz oder teilweise außerhalb der Geschäftsräume und Gebäude des Landkreises Lüchow-Dannenberg verrichtet wird.
Es wird mobiles Arbeiten angeboten, keine Telearbeit. S. INF.9 Mobiler Arbeitsplatz	

OPS.1.2.6 NTP-Zeitsynchronisation	
Beschreibung	Vernetzte IT-Systeme erfordern oftmals synchrone Zustände. Meist dient die Uhrzeit als Referenz. Die interne Uhr von IT-Systemen kann jedoch von der tatsächlichen Zeit abweichen. Das Network Time Protocol (NTP) wird dazu verwendet, regelmäßig eine Referenzzeit zentraler Zeitgeber über Netzverbindungen zu ermitteln und die interne Uhr entsprechend anzupassen.
Anforderungen	
OPS.1.2.6.A1 Planung des NTP- Einsatzes	• Der NTP-Einsatz ist geplant und im NTP-Konzept dokumentiert.
OPS.1.2.6.A2 Sichere Nutzung fremder Zeitquellen	• Als fremde Zeitquellen kommen folgende NTP-Server zum Einsatz: 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org,

	3.pool.ntp.org • Das pool.ntp.org Projekt ist ein großer virtueller Cluster aus Zeitservern, der verlässlich und auf einfache Weise Zeitsynchronisation über NTP für mehrere Millionen Computer zur Verfügung stellt.
OPS.1.2.6.A3 Sichere Konfiguration von NTP-Servern	• Es kommen keine internen NTP-Server zum Einsatz.
OPS.1.2.6.A4 Nichtberücksichtigung unaufgeforderter Zeitinformationen	• Auf allen relevanten Systemen wird die Uhrzeit zentral erzwungen. Zeitänderungen können nur von der zentralen Stelle durchgeführt werden.
OPS.1.2.6.A5 Nutzung des Client-Server-Modus für NTP	• Es kommen keine internen NTP-Server zum Einsatz.
OPS.1.2.6.A6 Überwachung von IT-Systemen mit NTP-Nutzung	• Sämtliche IT-Systeme werden über die Check_MK (Monitoring) überwacht. Hierbei werden sowohl Zeitabweichungen als auch ausgefallene Dienste gemeldet und protokolliert.
OPS.1.2.6.A7 Sichere Konfiguration von NTP-Clients	• Die sichere Konfiguration der NTP-Clients ergibt sich aus den Funktionen der Produkte.
OPS.1.2.6.A8 Einsatz sicherer Protokolle zur Zeitsynchronisation	• NTS kommt für den Landkreis Lüchow-Dannenberg derzeit nicht in Frage.

OPS.2.2 Cloud-Nutzung	
Beschreibung	Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz.
Keine Cloud-Nutzung mit Verarbeitung sicherheitsrelevanter Daten.	

OPS.3.2 Anbieten von Outsourcing	
Beschreibung	Beim Outsourcing lagern Institutionen (Nutzende von Outsourcing) Geschäftsprozesse oder Tätigkeiten ganz oder teilweise zu einem oder mehreren externen Dienstleistungsunternehmen (Anbietende von Outsourcing) aus. Diese sogenannten Anbietende von Outsourcing betreiben im Rahmen des vereinbarten Outsourcing-Verhältnisses die Geschäftsprozesse oder Tätigkeiten nach festgelegten Kriterien. Allerdings verbleibt die Verantwortung aus Sicht der Informationssicherheit stets bei der auslagernden Institution.
Kein Outsourcing.	

DER.1 Detektion von sicherheitsrelevanten Ereignissen	
Beschreibung	Um IT-Systeme schützen zu können, müssen sicherheitsrelevante Ereignisse rechtzeitig erkannt und behandelt werden. Dazu ist es notwendig, dass Institutionen im Vorfeld geeignete organisatorische, personelle und technische Maßnahmen planen, implementieren und regelmäßig üben Als sicherheitsrelevantes Ereignis wird ein Ereignis bezeichnet, das sich auf die Informationssicherheit auswirkt und die Vertraulichkeit, Integrität oder Verfügbarkeit beeinträchtigen kann.
Anforderungen	
DER.1.A2 Einhaltung rechtlicher Bedingungen bei der Auswertung von Protokollierungsdaten	• Die rechtlichen Bestimmungen werden bei der Auswertung von Protokollierungsdaten eingehalten.
DER.1.A3 Festlegung von Meldewegen für sicherheitsrelevante Ereignisse	• Der FD 16 startet den Meldeweg und informiert die ISB oder den ISB. Der FD 16 und die ISB oder der ISB informieren alle zu beteiligenden Personen bei einem Sicherheitsvorfall (Übersicht liegt dem FD 16 und der ISB vor) per Telefon und ggf. per Mail. • Die Übersicht der zu beteiligenden Personen wird bei Änderungen angepasst.

DER.1.A4 Sensibilisierung der Mitarbeitenden	• Die Mitarbeitenden werden durch regelmäßige Schulungen und aktuelle Informationen zur Sicherheitslage sensibilisiert.
DER.1.A12 Auswertung von Informationen aus externen Quellen	• Informationen von externen Quellen werden an die ISB oder den ISB und den FD 16 weitergeleitet.
DER.1.A13 Regelmäßige Audits der Detektionssysteme	• Regelmäßige Audits sind geplant.

DER.2.1 Behandlung von Sicherheitsvorfällen	
Beschreibung	Um Schäden zu begrenzen und um weitere Schäden zu vermeiden, müssen erkannte Sicherheitsvorfälle schnell und effizient bearbeitet werden. Dafür ist es notwendig, ein vorgegebenes und erprobtes Verfahren zur Behandlung von Sicherheitsvorfällen zu etablieren
Anforderungen	
DER.2.1.A1 Definition eines Sicherheitsvorfalls	• Ein Sicherheitsvorfall ist ein Ereignis, das die Informationssicherheit beeinträchtigt. Der Vorfall gefährdet die Sicherheitsziele Vertraulichkeit, Verfügbarkeit oder Integrität der Daten, IT-Anwendungen, IT-Systeme oder IT-Dienste. • Sicherheitsvorfälle sind so weit wie möglich von Störungen im Tagesbetrieb abzugrenzen.
DER.2.1.A2 Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen	• Die „Richtlinie zur Behandlung von Sicherheitsvorfällen für den Landkreis Lüchow-Dannenberg“ ist erstellt.
DER.2.1.A3 Festlegung von Verantwortlichkeiten und Ansprechpersonen bei Sicherheitsvorfällen	• Ansprechperson für die Mitarbeitenden bei einem vermuteten Sicherheitsvorfall ist der FD 16. Dieser informiert die ISB oder den ISB.
DER.2.1.A4 Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen	• Der FD 16 benachrichtigt die ISB oder den ISB. • FD 16 und ISB benachrichtigen die weiteren zu beteiligenden Stellen.
DER.2.1.A5 Behebung von Sicherheitsvorfällen	• Bei der Behebung von Sicherheitsvorfällen müssen FDL 16 und die oder der ISB die Freigabe erteilen, bevor entsprechende Maßnahmen umgesetzt werden. Eine Liste von zu beteiligenden Personen liegt vor.
DER.2.1.A6 Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen	• Die Wiederherstellung erfolgt entsprechend der „Richtlinie zur Behandlung von Sicherheitsvorfällen für den Landkreis Lüchow-Dannenberg“.
DER.2.1.A7 Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen	• Eine geeignete Vorgehensweise zur Behandlung von Sicherheitsvorfällen ist etabliert.
DER.2.1.A8 Aufbau von Organisationsstrukturen zur Behandlung von Sicherheitsvorfällen	• Der Krisenstab setzt sich zusammen aus der Verwaltungsleitung, FDL 16, der ISB oder dem ISB • ab Einstufung als Notfall zusätzlich: der DSB oder dem DSB, FDL 10 FGL Personal FGL Organisation Fachkommissariat Cybercrime Lüneburg ggf. die Pressestelle, ggf. den Personalrat, ggf. das Justitiariat. ggf. das BSI ggf. LKA Niedersachen ggf. ZAC (Zentrale Ansprechstelle Cybercrime) • bei einer Einstufung als Notfall zusätzlich: KatS
DER.2.1.A9 Festlegung von Meldewegen für	• Bei Auffälligkeiten in Bezug auf die

Sicherheitsvorfälle	Informationssicherheit ist unverzüglich der FD 16 (telefonisch: 05841 120 444 oder per E-Mail: Tanss@luechow-dannenberg.de) zu informieren. • Außerhalb der Servicezeiten des Service-Desk des FD 16 ist die IT-Notfallnummer zu wählen. Dadurch werden alle Kolleginnen und Kollegen des FD 16 und die bzw. der ISB auf ihren Smartphones benachrichtigt. • Der FD 16 informiert FDL 16 und die ISB oder den ISB, • FDL 16 und ISB informieren ggf.: der DSB oder dem DSB, die Verwaltungsleitung, FDL 10 FGL Personal FGL Organisation Fachkommissariat Cybercrime Lüneburg ggf. die Pressestelle, ggf. den Personalrat, ggf. das Justitiariat. ggf. das BSI ggf. LKA Niedersachen ggf. ZAC (Zentrale Ansprechstelle Cybercrime) KatS • Bei einem Verdacht auf einen Sicherheitsvorfall sind folgende Informationen an den FD 16 zu melden: Welches IT-System ist betroffen? Wie haben Sie mit dem IT-System gearbeitet? Was haben Sie beobachtet? Wann ist das Ereignis eingetreten? Wo befindet sich das betroffene IT-System? (Gebäude, Raum, Arbeitsplatz)
DER.2.1.A10 Eindämmen der Auswirkung von Sicherheitsvorfällen	• Für jeden Sicherheitsvorfall entscheidet das Sicherheitsvorfall-Team, ob es wichtiger ist, den entstandenen Schaden einzudämmen oder den Vorfall aufzuklären.
DER.2.1.A11 Einstufung von Sicherheitsvorfällen	• Ein einheitliches Verfahren zu Einstufung ist festgelegt (nach BSI-Standard).
DER.2.1.A12 Festlegung der Schnittstellen der Sicherheitsvorfallbehandlung zur Störungs- und Fehlerbehebung	• Bei jedem Sicherheitsvorfall und im Notfallmanagement sind der FD 16 und die ISB oder der ISB beteiligt.
DER.2.1.A13 Einbindung in das Sicherheits- und Notfallmanagement	• Die Behebung von Sicherheitsvorfällen ist mit dem Notfallmanagement abgestimmt.
DER.2.1.A14 Eskalationsstrategie für Sicherheitsvorfälle	• Die einzubeziehenden Beteiligten sind benannt. Der Kontakt zum FD 16 ist auch während eines Sicherheitsvorfalls gesichert.
DER.2.1.A15 Schulung der Mitarbeitenden des Service Desk	• Die Mitarbeitenden des FD 16 werden regelmäßig geschult.
DER.2.1.A16 Dokumentation der Behebung von Sicherheitsvorfällen	• Die Dokumentation der Behebung eines Sicherheitsvorfalls beinhaltet die durchgeführten Aktionen inkl. der Zeitpunkte, Protokolldateien und ggf. anderen Nachweisen.
DER.2.1.A17 Nachbereitung von Sicherheitsvorfällen	• Sicherheitsvorfälle sind standardisiert nachzubereiten. Dabei ist zu untersuchen, Wie schnell Sicherheitsvorfälle erkannt und behoben wurden, ob die Meldewege funktionierten, ausreichend Informationen für die Bewertung verfügbar waren und ob die Detektionsmaßnahmen wirksam waren.
DER.2.1.A18 Weiterentwicklung der Prozesse durch Erkenntnisse aus Sicherheitsvorfällen und Branchenentwicklungen	• Die Reaktionen auf Sicherheitsvorfälle werden regelmäßig analysiert und daraufhin untersucht, ob die Prozesse und Abläufe geändert oder

	weiterentwickelt werden müssen.

DER.2.2 Vorsorge für die IT-Forensik	
Beschreibung	IT-Forensik ist die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Datennetzen zur Aufklärung von Sicherheitsvorfällen in IT-Systemen.
Anforderungen	
DER 2.1.A1 Prüfung rechtlicher und regulatorischer Rahmenbedingungen zur Erfassung und Auswertbarkeit	• Die rechtlichen und regulatorischen Rahmenbedingungen sind identifiziert. Personalrat und die Datenschutzbeauftragte oder der Datenschutzbeauftragte werden bei der Erfassung und Auswertung von Daten für die IT-Forensik einbezogen.
DER.2.2.A2 Erstellung eines Leitfadens für Erstmaßnahmen bei einem IT-Sicherheitsvorfall	• Für den Landkreis Lüchow-Dannenberg ist ein Leitfaden für Erstmaßnahmen bei einem IT-Sicherheitsvorfall erstellt.
DER.2.2.A3 Vorauswahl von Forensik-Dienstleistenden	• Die IT-Forensik erfolgt durch das Fachkommissariat Cybercrime, Zentrale Kriminalinspektion Lüneburg.
DER.2.2.A4 Festlegung von Schnittstellen zum Krisen- und Notfallmanagement	• Kontaktpersonen für die IT-Forensik sind die Notfallbeauftragte oder der Notfallbeauftragte und die FDL 16.
DER.2.2.A5 Erstellung eines Leitfadens für Beweissicherungsmaßnahmen bei IT-Sicherheitsvorfällen	• Die IT-Forensik erfolgt durch das Fachkommissariat Cybercrime, Zentrale Kriminalinspektion Lüneburg.
DER.2.2.A6 Schulung des Personals für die Umsetzung der forensischen Sicherung	• Die IT-Forensik erfolgt durch das Fachkommissariat Cybercrime, Zentrale Kriminalinspektion Lüneburg.
DER.2.2.A7 Auswahl von Werkzeugen zur Forensik	• Die IT-Forensik erfolgt durch das Fachkommissariat Cybercrime, Zentrale Kriminalinspektion Lüneburg.
DER.2.2.A8 Auswahl und Reihenfolge der zu sichernden Beweismittel	• Die IT-Forensik erfolgt durch das Fachkommissariat Cybercrime, Zentrale Kriminalinspektion Lüneburg.
DER.2.2.A9 Vorauswahl forensisch relevanter Daten	• Log-Daten werden für ein halbes Jahr gesichert.
DER.2.2.A10 IT-forensische Sicherung von Beweismitteln	• Die IT-Forensik erfolgt durch das Fachkommissariat Cybercrime, Zentrale Kriminalinspektion Lüneburg.
DER.2.2.A11 Dokumentation der Beweissicherung	• Die IT-Forensik erfolgt durch das Fachkommissariat Cybercrime, Zentrale Kriminalinspektion Lüneburg.
DER.2.2.A12 Sichere Verwahrung von Originaldatenträgern und Beweismitteln	• Die IT-Forensik erfolgt durch das Fachkommissariat Cybercrime, Zentrale Kriminalinspektion Lüneburg.

DER.3.1 Audits und Revisionen	
Beschreibung	Audits und Revisionen sind ein Werkzeug, um ein angemessenes Sicherheitsniveau festzustellen, zu erreichen und aufrechtzuerhalten. Durch Audits und Revisionen ist es möglich, Sicherheitsmängel und Fehlentwicklungen zu erkennen und entsprechende Gegenmaßnahmen zu ergreifen.
Anforderungen	
DER.3.1.A1 Definition von Verantwortlichkeiten	• Audits bzw. Revisionen werden von der ISB oder dem ISB und dem FD 16 geplant.
DER.3.1.A2 Vorbereitung eines Audits oder einer Revision	• Vor einem Audit oder einer Revision werden Prüfgegenstand und Prüfungsziele festgelegt. Vor einem Audit oder einer Revision werden die zuständige Organisationseinheit und der Personalrat informiert.
DER.3.1.A3 Durchführung eines Audits	• Es werden ausschließlich externe Audits

	durchgeführt, da kein unabhängiges Personal für ein Auditteam vorhanden ist. • Die dazugehörigen Anforderungen sind bekannt.
DER.3.1.A4 Durchführung einer Revision	• Es werden ausschließlich externe Revisionen durchgeführt, da kein unabhängiges Personal für ein Revisionsteam vorhanden ist. • Festgestellte Abweichungen werden schnellstmöglich korrigiert.
DER.3.1.A5 Integration in den Informationssicherheitsprozess	• Es werden ausschließlich externe Audits durchgeführt, da kein unabhängiges Personal für ein Auditteam vorhanden ist. • Die Ergebnisse werden von der ISB oder dem ISB in das ISMS integriert und der Verwaltungsleitung in den Quartalsberichten bekannt gegeben.
DER.3.1.A6 Definition der Prüfungsgrundlage und eines einheitlichen Bewertungsschemas	• Es werden ausschließlich externe Audits durchgeführt, da kein unabhängiges Personal für ein Auditteam vorhanden ist.
DER.3.1.A7 Erstellung eines Auditprogramms	• Es werden ausschließlich externe Audits durchgeführt, da kein unabhängiges Personal für ein Auditteam vorhanden ist. • Für jedes Audit/jede Revision werden Ziele festgelegt. • Ressourcen für unvorhersehbare Ereignisse werden in der jährlichen Haushaltsplanung berücksichtigt.
DER.3.1.A8 Erstellung einer Revisionsliste	• Eine Revisionsliste liegt vor.
DER.3.1.A9 Auswahl eines geeigneten Audit- oder Revisionsteams	• Es werden ausschließlich externe Audits und Revisionen durchgeführt, da kein unabhängiges Personal für ein Audit-/Revisionsteam vorhanden ist.
DER.3.1.A10 Erstellung eines Audit- oder Revisionsplans	• Es werden ausschließlich externe Audits und Revisionen durchgeführt, da kein unabhängiges Personal für ein Audit-/Revisionsteam vorhanden ist.
DER.3.1.A11 Kommunikation und Verhalten während der Prüfungen	• Vor Audits und Revisionen werden die Kommunikationswege festgelegt.
DER.3.1.A12 Durchführung eines Auftaktgesprächs	• Es werden ausschließlich externe Audits und Revisionen durchgeführt, da kein unabhängiges Personal für ein Audit-/Revisionsteam vorhanden ist.
DER.3.1.A13 Sichtung und Prüfung der Dokumente	• Es werden ausschließlich externe Audits und Revisionen durchgeführt, da kein unabhängiges Personal für ein Audit-/Revisionsteam vorhanden ist.
DER.3.1.A14 Auswahl von Stichproben	• Es werden ausschließlich externe Audits und Revisionen durchgeführt, da kein unabhängiges Personal für ein Audit-/Revisionsteam vorhanden ist.
DER.3.1.A15 Auswahl von geeigneten Prüfmethoden	• Es werden ausschließlich externe Audits und Revisionen durchgeführt, da kein unabhängiges Personal für ein Audit-/Revisionsteam vorhanden ist.
DER.3.1.A16 Ablaufplan der Vor-Ort-Prüfung	• Es werden ausschließlich externe Audits und Revisionen durchgeführt, da kein unabhängiges Personal für ein Audit-/Revisionsteam vorhanden ist.
DER.3.1.A17 Durchführung der Vor-Ort-Prüfung	• Es werden ausschließlich externe Audits und Revisionen durchgeführt, da kein unabhängiges Personal für ein Audit-/Revisionsteam vorhanden ist.
DER.3.1.A18 Durchführung von Interviews	• Es werden ausschließlich externe Audits und Revisionen durchgeführt, da kein unabhängiges Personal für ein Audit-/Revisionsteam vorhanden ist.

DER.3.1.A19 Überprüfung des Risikobehandlungsplans	• Es werden ausschließlich externe Audits und Revisionen durchgeführt, da kein unabhängiges Personal für ein Audit-/Revisionsteam vorhanden ist.
DER.3.1.A20 Durchführung einer Abschlussbesprechung	• Es werden ausschließlich externe Audits und Revisionen durchgeführt, da kein unabhängiges Personal für ein Audit-/Revisionsteam vorhanden ist.
DER.3.1.A21 Auswertung der Prüfungen	• Es werden ausschließlich externe Audits und Revisionen durchgeführt, da kein unabhängiges Personal für ein Audit-/Revisionsteam vorhanden ist.
DER.3.1.A22 Erstellung eines Auditberichts	• Es werden ausschließlich externe Audits und Revisionen durchgeführt, da kein unabhängiges Personal für ein Audit-/Revisionsteam vorhanden ist.
DER.3.1.A23 Dokumentation der Revisionsergebnisse	• Es werden ausschließlich externe Audits und Revisionen durchgeführt, da kein unabhängiges Personal für ein Audit-/Revisionsteam vorhanden ist.
DER.3.1.A24 Abschluss des Audits oder der Revision	• Es werden ausschließlich externe Audits und Revisionen durchgeführt, da kein unabhängiges Personal für ein Audit-/Revisionsteam vorhanden ist.
DER.3.1.A25 Nachbereitung eines Audits	• Festgestellte Abweichungen werden priorisiert und durch geeignete Maßnahmen behoben. Die Korrekturmaßnahmen werden dokumentiert und überprüft.
DER.3.1.A26 Überwachen und Anpassen des Auditprogramms	• Das Auditprogramm wird überwacht und ggf. angepasst.
DER.3.1.A27 Aufbewahrung und Archivierung von Unterlagen zu Audits und Revisionen	• Die Unterlagen werden revisionssicher im DMS abgelegt und nach Erreichen der Aufbewahrungsfrist vernichtet.

DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision	
Beschreibung	Eine besondere Form der Revision ist die Informationssicherheitsrevision (IS-Revision) auf Basis des Dokuments Informationssicherheitsrevision – Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz (kurz „Leitfaden IS-Revision"). Der „Leitfaden IS-Revision" ist ein vom BSI veröffentlichtes Dokument, das die Vorgehensweise der IS-Revision beschreibt.
IS-Revisionen entsprechend des Leitfadens werden nicht durchgeführt.	

DER.4 Notfallmanagement	
Beschreibung	In Notfällen müssen Institutionen weiter auf Informationen zugreifen können, um einen Geschäftsprozess, ein IT-System oder eine Fachaufgabe wiederherstellen zu können. Um die Informationssicherheit auch in einem Notfall aufrechterhalten zu können, sollten deshalb entsprechende Prozesse geplant, etabliert und überprüft werden.
Anforderungen	
DER.4.A2 Integration von Notfallmanagement und Informationssicherheitsmanagement	• Die Prozesse des Informationssicherheitsmanagement werden mit dem Notfallmanagement abgestimmt.

6. System-Bausteine

APP = Anwendungen
SYS = IT-Systeme

NET = Netze und Kommunikation
INF = Infrastruktur

APP.1.4 Mobile Anwendungen (Apps)	
Beschreibung	Ziel dieses Bausteins ist es, Informationen zu schützen, die auf mobilen Endgeräten mit Apps verarbeitet werden. Auch die Einbindung von Apps in eine bestehende IT-Infrastruktur wird dabei betrachtet. Der Baustein definiert zudem Anforderungen, um Apps richtig auszuwählen und sicher betreiben zu können. Dabei werden die Apps unabhängig von ihrer Quelle (App Store oder eigene Installation) betrachtet.
Anforderungen	
APP.1.4.A1 Anforderungsanalyse für die Nutzung von Apps	• Ist durch die Nutzung der MDM-Lösung (Relution) gewährleistet. Die Geräte sind voll verwaltet und können auch jederzeit gesperrt oder gelöscht werden.
APP.1.4.A5 Minimierung und Kontrolle von App-Berechtigungen	• Ist durch die Nutzung der MDM-Lösung (Relution) gewährleistet. Berechtigungen werden hierüber gesteuert.
APP.1.4.A3 Verteilung schutzbedürftiger Apps	• Ist durch die Nutzung der MDM-Lösung (Relution) gewährleistet. • Apps werden hier nur von dem FD 16 freigegeben und in einem extra App Store veröffentlicht.
APP.1.4.A12 Sichere Deinstallation von Apps	• Ist durch die Nutzung der MDM-Lösung (Relution) gewährleistet.

APP.2.1 Allgemeiner Verzeichnisdienst	
Beschreibung	Ziel dieses Bausteins ist es, allgemeine Verzeichnisdienste sicher zu betreiben sowie die damit verarbeiteten Informationen angemessen zu schützen.
Als Verzeichnisdienst wird ausschließlich der AD genutzt. Dieser wird in APP 2.2 beschrieben.	

APP.2.2 Active Directory Domain Services	
Beschreibung	Das Ziel dieses Bausteins ist es, Active Directory Domain Services im Regelbetrieb einer Institution abzusichern, die AD DS zur Verwaltung von Windows-Systemen (Client und Server) sowie zur zentralen Authentifizierung und Autorisierung einsetzt.
Anforderungen	
APP.2.2.A5 Absicherung des Domänencontrollers	• Auf dem Domänencontroller laufen keine weiteren Dienste. • Die Möglichkeit des Restore über DSRM ist gegeben. • Die Protokollierung ist durch den Logserver gewährleistet.
APP.2.2.A6 Sichere Konfiguration von Vertrauensbeziehungen	• Es gibt eine „Vertrauensbeziehung“ (Vertrauensstellung) mit der Samtgemeinde Elbtalaue. Die Notwendigkeit ist durch gemeinsame Nutzungen gegeben.
APP.2.2.A16 Härtung der AD-DS-Konten	• Die Härtung findet über das Tool „PingCastle“ statt. Dieses Tool gibt Informationen darüber, welches Build-In-Konto aktiviert ist und wo die Passwörter sind. • Auch das AdminSDHolder-Objekt wird durch PingCastle geprüft und mitgeteilt.
APP.2.2.A18 Einschränken des Hinzufügens neuer Computer-Objekte zur Domäne	• Die Berechtigung, in der Domäne neue Computer-Objekte hinzuzufügen, ist auf die notwendigen administrativen Konten beschränkt.

APP.2.3 OpenLDAP	
Beschreibung	OpenLDAP ist ein frei verfügbarer Verzeichnisdienst, der in einem Datennetz Informationen über beliebige Objekte, beispielsweise Konten, IT-Systeme oder Konfigurationen, in einer standardisierten und definierten Art zur Verfügung stellt. Die Informationen können einfache Attribute wie die Namen oder Nummern von Objekten oder auch komplexe Formate wie Fotos oder Zertifikate für elektronische Signaturen umfassen. Typische Einsatzgebiete sind zum Beispiel Adressbücher oder Kontenverwaltungen, aber auch Konfigurationen.
Wird nicht genutzt.	

APP.3.3 Fileserver	
Beschreibung	Ein Fileserver (oder auch Dateiserver) ist ein Server in einem Netz, der Dateien von (internen) Festplatten oder Netzfestplatten für alle zugriffsberechtigten Personen sowie Clients zentral bereitstellt. Die Datenbestände können von den Zugriffsberechtigten genutzt werden, ohne sie z. B. auf Wechseldatenträgern zu transportieren oder per E-Mail zu verteilen. Dadurch, dass die Daten zentral vorgehalten werden, können sie strukturiert und in verschiedenen Verzeichnissen und Dateien bereitgestellt werden. Bei Fileservern können Zugriffsrechte auf die Dateien zentral vergeben werden. Auch die Datensicherung kann vereinfacht werden, wenn sich alle Informationen an einer zentralen Stelle befinden.
Anforderungen	
APP.3.3.A2 Einsatz von RAID-Systemen	• Die Anforderungen sind im Filesystem gegeben.
APP.3.3.A3 Einsatz von Viren-Schutzprogrammen	• flächendeckender Einsatz von TrendMicro und SecuLution im gesamten Netzwerk
APP.3.3.A15 Planung von Fileservern	• Der Fileserver ist virtuell und bezieht seine Speicherressourcen somit aus einem Netzwerkspeicher, welcher beliebig erweiterbar ist und mit ausreichend Reserven vorgehalten wird.
APP.3.3.A6 Beschaffung eines Fileservers und Auswahl eines Dienstes	• Der Fileserver ist virtuell. Die Ressourcen (Rechenleistung etc.) können je nach Bedarf jederzeit angepasst werden.
APP.3.3.A7 Auswahl eines Dateisystems	• Das Dateisystem wird über Berechtigungen gesteuert. Eine gesonderte Bewertung der Dateisysteme ist somit nicht notwendig. Die Schutzmechanismen des Windows-Betriebssystem werden auf dem Fileserver genutzt. Ein zeitgleiches Arbeiten an Dateien ist dadurch nicht möglich.
APP.3.3.A8 Strukturierte Datenhaltung	• Die Programm- und Arbeitsdaten sind voneinander getrennt. • Eine lokale Ablage von Daten ist nicht gewünscht. • Die Daten sollen zentral im DMS nscale abgelegt werden. • Die bestehenden Serverordner haben entsprechende Berechtigungen.
APP.3.3.A9 Sicheres Speichermanagement	• Der Fileserver bezieht seine Ressourcen aus den Netzwerkspeichern. • Der Netzwerkspeicher hat ein Monitoring und befindet sich in der Überwachung. Somit ist gewährleistet, dass die Speicher funktionsfähig und in gutem Zustand sind.
APP.3.3.A11 Einsatz von Speicherbeschränkungen	• Es gibt keine Begrenzungen vom Speicherplatz und somit auch keine Notwendigkeit für einen Füllstand.
APP.3.3.A14 Einsatz von Error-Correction-Codes	• Die ECC-Funktion von Windows ist auf dem Fileserver nicht aktiv. Da die Ressourcen sich aber aus einem Netzwerkspeicher

	(FlashSystem) beziehen, gibt es an dieser Stelle Mechanismen die das Dateisystem laufend überwachen und prüfen.

APP.3.4 Samba	
Beschreibung	Samba ist ein frei verfügbarer und vollwertiger Active Directory Domain Controller (ADDC), der Authentisierungs-, Datei- und Druckdienste bereitstellen kann und dadurch die Interoperabilität zwischen der Windows- und der Unix-Welt ermöglicht. Samba führt viele unterschiedliche Protokolle und Techniken zusammen. Dazu gehört beispielsweise das Server-Message-Block (SMB)-Protokoll. Als Samba-Server werden Server bezeichnet, auf denen Samba betrieben wird. In der Regel sind das Unix-Server.
Wird nicht genutzt.	

APP.4.2 SAP-ERP-System	
Beschreibung	Enterprise-Resource-Planning-Systeme von SAP (kurz SAP-ERP-Systeme) werden eingesetzt, um interne und externe Geschäftsabläufe zu automatisieren und technisch zu unterstützen. SAP-ERP-Systeme verarbeiten daher typischerweise vertrauliche Informationen, sodass alle Komponenten und Daten geeignet geschützt werden müssen.
Wird nicht genutzt.	

APP.4.4 Kubernetes	
Beschreibung	Kubernetes hat sich als De-Facto-Standard für die Orchestrierung von Containern in der Public und Private Cloud etabliert. Auch für IoT und andere Anwendungsfälle ist Kubernetes im Einsatz.
Wird nicht genutzt.	

APP.4.6 SAP ABAP-Programmierung	
Beschreibung	Häufig werden in SAP-Systemen Eigenentwicklungen programmiert. Die Gründe dafür sind vielfältig, so können Geschäftsprozesse oder Anforderungen an das Reporting mit Hilfe von Eigenentwicklungen individuell an die Institution angepasst werden. Außerdem ist es möglich, spezielle Funktionen zu erstellen, die in der Standard-Auslieferung nicht vorhanden sind.
Wird nicht genutzt.	

APP.5.2 Microsoft Exchange und Outlook	
Beschreibung	Microsoft Exchange Server (im Folgenden „Exchange“) ist eine Groupware-Lösung für mittlere bis große Institutionen. Mit ihr können elektronisch Nachrichten übermittelt werden und sie verfügt über weitere Dienste, um Workflows zu unterstützen. Nachrichten, wie E-Mails, können mit Exchange zentral verwaltet, zugestellt, gefiltert und versendet werden. Ebenso können typische Groupware-Anwendungen, wie Notizen, Kontaktlisten, Kalender und Aufgabenlisten angeboten und verwaltet werden. Um die Funktionen von Exchange nutzen zu können, ist neben dem Server-Dienst eine zusätzliche Client-Software oder ein Webbrowser nötig. Microsoft Outlook (im Folgenden „Outlook“) ist ein Client für Exchange, der durch die Installation des Office-Pakets von Microsoft oder durch Integration in die Betriebssysteme von mobilen Geräten direkt zur Verfügung gestellt wird. Darüber hinaus ermöglicht die Webanwendung „Outlook im Web“ (ehemals „Outlook Web App“) über den Browser z. B. auf E-Mails, Kontakte und den Kalender

	zuzugreifen. Diese Funktion ist in Exchange bereits enthalten. Die Kombination aus Exchange-Servern und Outlook-Clients wird in diesem Baustein als Exchange-System bezeichnet.
Anforderungen	
APP.5.2.A1 Planung des Einsatzes von Exchange und Outlook	• Die Migration von IBM-Notes zu Outlook wurde sorgfältig geplant und umgesetzt.
APP.5.2.A2 Auswahl einer geeigneten Exchange-Infrastruktur	• Die Planungen wurden gemeinsam mit einem Dienstleister beim Umstieg von IBM-Notes auf Exchange gemacht und durchgeführt. Es wurde sich für eine lokale on-premise-Lösung von Exchange entschieden.
APP.5.2.A5 Datensicherung von Exchange	• Der Exchange-Server ist im Datensicherungskonzept enthalten.
APP.5.2.A7 Migration von Exchange-Systemen	• Bislang mussten keine Migrationen innerhalb von Exchange durchgeführt werden.
APP.5.2.A10 Sichere Konfiguration von Outlook	• Es werden die Standardkonfigurationen von Outlook genutzt.
APP.5.2.A12 Einsatz von Outlook Anywhere, MAPI over HTTP und Outlook im Web	• Der Zugriff über das Internet ist auf wenige Mitarbeitende beschränkt. Die Zugänge von außerhalb sind über gesicherte Wege konfiguriert.

APP.5.3 Allgemeiner E-Mail-Client und –Server	
Beschreibung	E-Mail ist eine der am häufigsten genutzten und ältesten Internetanwendungen. E-Mails werden dazu verwendet, Texte und angehängte Dateien zu versenden. Dazu wird eine E-Mail-Adresse benötigt. Um E-Mail nutzen zu können, werden E-Mail-Server benötigt, die elektronische Nachrichten empfangen und versenden. In der Regel rufen E-Mail-Clients, mit denen auf E-Mail-Dienste zugegriffen wird, Nachrichten, die für sie bestimmt sind, mittels der Protokolle POP3 oder IMAP vom E-Mail-Server ab und senden mit dem Protokoll SMTP selbst Nachrichten an den E-Mail-Server, der diese bei Bedarf an einen anderen E-Mail-Server weiterleitet.
Anforderungen	
APP.5.3.A1 Sichere Konfiguration der E-Mail-Clients	• E-Mail-Client ist ausschließlich Outlook (s. APP 5.2).
APP.5.3.A2 Sicherer Betrieb von E-Mail-Servern	• E-Mail-Client ist ausschließlich Outlook (s. APP 5.2).
APP.5.3.A3 Datensicherung und Archivierung von E-Mails	• E-Mail-Client ist ausschließlich Outlook (s. APP 5.2).
APP.5.3.A4 Spam- und Virenschutz auf dem E-Mail-Server	• E-Mail-Client ist ausschließlich Outlook (s. APP 5.2).
APP.5.3.A7 Schulung zu Sicherheitsmechanismen von E-Mail-Clients für Benutzende	• Die Mitarbeitenden werden regelmäßig zu Risiken und Gefahren sowie zum Erkennen von Spam-Mails geschult.
APP.5.3.A8 Umgang mit Spam durch Benutzende	• Spam-Mails sollen direkt gelöscht werden. Bei Unsicherheiten ist Rücksprache mit dem FD 16 oder der bzw. dem ISB zu halten.

APP.5.4 Unified Communications und Collaboration (UCC)	
Beschreibung	Unified Communications bezeichnet einen Dienst, der verschiedene Kommunikationsdienste in einer Anwendung und in der Regel auch einem Softclient vereint. Damit wird der Anteil der traditionellen Telefonie in der persönlichen digitalen Kommunikation reduziert. Die möglichen Kommunikationswege werden um zusätzliche Dienste wie Video, diverse Formen von Chats und Erreichbarkeitsanzeigen erweitert.
Wird nicht genutzt.	

APP.6 Allgemeine Software	
Beschreibung	Dieser Baustein fasst jegliche Software unter dem Begriff Allgemeine Software zusammen, unabhängig davon, ob es sich um eine Textverarbeitung, ein Betriebssystem, eine mobile Kommunikations-App, eine individuell entwickelte Software oder ein verteiltes Content-Management-System handelt.
Anforderungen	
APP.6.A1 Planung des Software-Einsatzes	• Vor Einsatz einer Software wird geplant, wofür diese genutzt werden soll und welche Informationen verarbeitet werden sollen. • Die Einführung in den Organisationseinheiten erfolgt durch die jeweiligen Fachadministratorinnen bzw. Fachadministratoren und der Führungskraft mit Unterstützung durch den FD 16. • Die technische Umsetzung erfolgt durch den FD 16. • Die Freigabe der bzw. des ISB und der bzw. des DSB sind ebenfalls erforderlich. • Die fachliche Betreuung erfolgt durch die jeweiligen Fachadministratorinnen bzw. Fachadministratoren der Organisationseinheit. • Die technische Betreuung übernimmt der FD 16.
APP.6.A2 Erstellung eines Anforderungskatalogs für Software	• Die Anforderungen an die Software legt die jeweilige Organisationseinheit fest. Dabei ist Rücksprache mit dem FD 16, der bzw. dem ISB und der bzw. dem DSB zu halten.
APP.6.A3 Sichere Beschaffung von Software	• Die Beschaffung inkl. Wartungsvereinbarungen erfolgt durch den FD 16.
APP.6.A6 Berücksichtigung empfohlener Sicherheitsanforderungen	• Folgende Sicherheitsanforderungen werden bei der Beschaffung von Software berücksichtigt: - Die Software sollte generelle Sicherheitsfunktionen wie Protokollierung und Authentifizierung umfassen, die im Anwendungskontext erforderlich sind. - Die Software sollte es ermöglichen, die Härtungsfunktionen der Einsatzumgebung zu nutzen. Hierbei sollten insbesondere die Härtungsfunktionen des geplanten Betriebssystems und der geplanten Ausführungsumgebung berücksichtigt werden. - Wenn durch die Software Informationen über ungesicherte, öffentliche Netze übertragen werden, dann sollte die Software sichere Verschlüsselungsfunktionen einsetzen, die dem Stand der Technik entsprechen. Darüber hinaus sollten die übertragenen Daten auf Integrität überprüft werden, indem Prüfsummen oder digitale Signaturen eingesetzt werden. - Verwendet die Software Zertifikate, dann sollte sie die Möglichkeit bieten, die Zertifikate transparent darzustellen. Zudem sollte es möglich sein, Zertifikate zu sperren, ihnen das Vertrauen zu entziehen oder eigene Zertifikate zu ergänzen.
APP.6.A7 Auswahl und Bewertung potentieller Software	• Die Auswahl und Bewertung von Software erfolgt im Vergabeverfahren.
APP.6.A10 Erstellung einer Sicherheitsrichtlinie für den Einsatz der Software	• Einsatz und Betrieb der Software wird in den

	Organisationseinheiten dokumentiert. • Die Dokumentation wird nach Bedarf aktualisiert.
APP.6.A12 Geregelte Außerbetriebnahme von Software	• Eine Außerbetriebnahme erfolgt durch Absprache zwischen der Organisationseinheit und dem FD 16. • Die Benutzenden werden rechtzeitig informiert.

APP.7 Entwicklung von Individualsoftware	
Beschreibung	Viele Institutionen stehen vor Herausforderungen, die sie nicht mehr hinreichend mit unangepasster Software lösen können. Die mit diesen Herausforderungen verbundenen Aufgabenstellungen bedürfen häufig Softwarelösungen, die auf die individuellen Bedürfnisse der Institutionen zugeschnitten sind. Im Folgenden werden diese Softwarelösungen als Individualsoftware bezeichnet. Hierzu können einerseits Basislösungen, die aus einer Grundmenge an typischen Funktionen bestehen, eingesetzt und individualisiert werden. Die Grundfunktionen werden hierbei für den individuellen Einsatzzweck der Institution angepasst und um individuell benötigte Funktionen erweitert. Gängige Beispiele hierfür sind IT-Anwendungen wie ERP- (Enterprise Resource Planning), CMS- (Content Management Systeme) oder IDM-Systeme (Identity Management). Individualsoftware kann auch vollständig neu von der Institution selbst oder von Dritten entwickelt werden.
Es wird keine Individualsoftware entwickelt.	

SYS.1.2.2 Windows Server 2012	
Beschreibung	Mit Windows Server 2012 hat Microsoft im September 2012 ein Betriebssystem für Server auf den Markt gebracht, das diverse Verbesserungen der Sicherheit gegenüber bisherigen Windows-Versionen, insbesondere auch gegenüber dem Vorgänger Windows Server 2008 R2, mitbringt.
Wird nicht genutzt.	

SYS.1.6 Containerisierung	
Beschreibung	Der Begriff Containerisierung bezeichnet ein Konzept, bei dem Ressourcen eines Betriebssystems partitioniert werden, um Ausführungsumgebungen für Prozesse zu schaffen.
Wird nicht genutzt.	

SYS.1.7 IBM Z	
Beschreibung	Systeme vom Typ „IBM Z" gehören zu den Server-Systemen, die allgemein als Großrechner („Mainframes") bezeichnet werden.
Wird nicht genutzt.	

SYS.2.3 Clients unter Linux und Unix	
Beschreibung	Neben Windows werden auf immer mehr Clients Linux- oder seltener Unix-basierte Betriebssysteme installiert.
Wird nicht genutzt.	

SYS.2.4 Clients unter macOS	
Beschreibung	macOS ist ein Client-Betriebssystem der Firma Apple. macOS basiert auf Darwin, dem frei verfügbaren Unix-Betriebssystem von Apple, das wiederum auf dem Open-Source-Betriebssystem FreeBSD aufbaut.
Wird nicht genutzt.	

SYS.3.2.1 Allgemeine Smartphones und Tablets	
Beschreibung	Smartphones sind auf den mobilen Einsatz ausgerichtete IT-Systeme mit einer angepassten Oberfläche, die mit einem großen, üblicherweise berührungsempfindlichen Bildschirm (Touch-Display) bedient werden können. Smartphones vereinen neben der Telefonie beispielsweise Media-Player, Personal Information Manager und Digitalkamera in einem Gerät und bieten den Benutzenden darüber hinaus viele weitere Anwendungen und Funktionen, wie Webbrowser, E-Mail-Client oder Ortung (z. B. über GPS). Zudem sind sie mit Mobilfunk-, WLAN-, Bluetooth- sowie NFC-Schnittstellen ausgestattet. Tablets sind, vereinfacht gesagt, Smartphones mit großem Formfaktor, mit denen in der Regel nicht über das Mobilfunknetz telefoniert werden kann.
Anforderungen	
SYS.3.2.1.A7 Verhaltensregeln bei Sicherheitsvorfällen	• Bei Verlust eines Geräts oder Verdacht auf einen Informationssicherheitsvorfall ist unverzüglich der FD 16 zu informieren.

SYS.3.2.3 iOS (for Enterprise)	
Beschreibung	Aufgrund von modernen, einfachen Bedienkonzepten sowie ihrer hohen Leistungsfähigkeit sind Smartphones und Tablets heutzutage weit verbreitet. Dazu zählen auch die von der Firma Apple produzierten Mobilgeräte iPhone und iPad mit den Betriebssystemen iOS und iPadOS.
Wird nicht genutzt.	

SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte	
Beschreibung	Moderne Drucker, Kopierer und Multifunktionsgeräte sind komplexe Geräte, die neben mechanischenKomponenten eigene Betriebssysteme enthalten und Serverdienste und -funktionen bereitstellen. Da die Geräte oft vertrauliche Informationen verarbeiten, müssen sie bzw. die gesamte Druck- und Scan-Infrastruktur geschützt werden.Als Multifunktionsgeräte werden Geräte bezeichnet, die mehrere papierverarbeitende Funktionen bieten, etwa Drucken, Kopieren, Scannen sowie auch Versenden und Empfangen von Fax-Dokumenten.
Anforderungen	
SYS.4.1.A22 Ordnungsgemäße Entsorgung ausgedruckter Dokumente	• Alle ausgedruckten Dokumente mit vertraulichen Informationen sind in den Mülleimern der Büros zu entsorgen, damit diese geeignet geschreddert werden.

SYS.4.4 Allgemeines IoT-Gerät	
Beschreibung	Geräte mit Funktionen aus dem Bereich Internet of Things (IoT) sind, im Gegensatz zu klassischen Endgeräten, vernetzte Geräte oder Gegenstände, die zusätzliche „smarte" Funktionen besitzen. IoT-Geräte werden in der Regel drahtlos an Datennetze angeschlossen. Die meisten Geräte können auf Informationen im Internet zugreifen und darüber erreicht werden. Hierdurch können sie Auswirkungen auf die Informationssicherheit des gesamten Informationsverbunds haben.
Wird nicht genutzt.	

SYS.4.5 Wechseldatenträger	
Beschreibung	Wechseldatenträger werden oft eingesetzt, um Daten zu transportieren, zu speichern oder um mobil auf sie zugreifen zu können. Zu Wechseldatenträgern gehören externe Festplatten, CD-ROMs, DVDs, Speicherkarten, Magnetbänder und USB-Sticks. Wechseldatenträger sind danach klassifizierbar, ob sie nur lesbar, einmalig beschreibbar oder wiederbeschreibbar sind. Unterschiede gibt es auch bei der Art der Datenspeicherung (analog oder digital) oder ihrer Bauform. So gibt es auswechselbare Datenträger (z. B. verbaute Festplatten) oder externe Datenspeicher (z. B. USB-Sticks).
Anforderungen	
SYS.4.5.A1 Sensibilisierung zum sicheren Umgang mit Wechseldatenträgern	• Die Sensibilisierung erfolgt im Rahmen der jährlichen Informationssicherheitsschulung.
SYS.4.5.A2 Verlust- und Manipulationsmeldung	• Die Mitarbeitenden haben bei dem Verlust eines Wechseldatenträgers oder bei Verdacht einer Manipulation unverzüglich den FD 16 zu informieren. • In den Diensträumen aufgefundene Wechseldatenträger sind ebenfalls beim FD 16 abzugeben.

INF.1 Allgemeines Gebäude	
Beschreibung	Ein Gebäude umschließt alle stationären Arbeitsplätze, die verarbeiteten Informationen sowie die aufgestellte Informationstechnik. Es gewährleistet somit einen Schutz vor äußeren Einflüssen. Daher ist nicht nur das Bauwerk an sich zu betrachten, also Wände, Decken, Böden, Dach, Fenster sowie Türen, sondern auch alle gebäudeweiten Infrastruktur- und Versorgungseinrichtungen wie Strom, Wasser, Gas, Heizung und Kühlung.
Anforderungen	
INF.1.A1 Planung der Gebäudeabsicherung	• Zutrittsregelungen sind erfolgt. • Der FD 16-Sicherheitsbereich ist gesondert abgesichert. • Brandschutztüren sind vorhanden. • Versammlungsorte sind bekannt und ausgeschildert.
INF.1.A6 Geschlossene Fenster und Türen	• Türen sind bei Verlassen des Raums zu verschließen. • Fenster und Türen sind bei Verlassen des Gebäudes zu verschließen.
INF.1.A8 Rauchverbot	• In den Gebäuden des Landkreises Lüchow-Dannenberg herrscht Rauchverbot.

INF.2 Rechenzentrum sowie Serverraum	
Beschreibung	Der vorliegende Baustein eignet sich nicht für kleine Informationsverbünde mit z. B. nur einem oder sehr wenigen Servern oder IT-Systemen. Ein Beispiel dafür ist eine kleine Institution mit wenigen IT-Arbeitsplätzen und einem Server, der in einem separaten Raum betrieben wird. In solchen Fällen genügt es oft, den Baustein INF.5 Raum sowie Schrank für technische Infrastruktur umzusetzen.
Es existieren lediglich ein kleiner Raum mit zwei Schränken und kleine Verteilerräume in den verschiedenen Gebäudeteilen.	

INF.7 Büroarbeitsplatz	
Beschreibung	Ein Büroraum ist der Bereich innerhalb einer Institution, in dem sich ein oder mehrere Mitarbeitende aufhalten, um dort ihre Aufgaben zu erfüllen.
Anforderungen	

INF.7.A1 Geeignete Auswahl und Nutzung eines Büroraumes	• Die FG Organisation des FD 10 kümmert sich um die Verteilung der Büroräume.
INF.7.A2 Geschlossene Fenster und abgeschlossene Türen	• Die Türen sind bei Verlassen des Büroraums zu verschließen. • Die Fenster im Erdgeschoss dürfen beim Verlassen des Büroraums nicht weit geöffnet bleiben. • Die Fenster sind bei längerer Abwesenheit, z.B. bei Außendiensten oder Feierabend, vollständig zu schließen. • Brand- und Rauchschutztüren müssen geschlossen werden.
INF.7.A3 Fliegende Verkabelung	• Stromanschlüsse und Zugänge zum Datenschutz befinden sich in der Nähe der IT-Geräte. • Verkabelungen die über den Boden verlaufen, sollten geeignet abgedeckt werden.
INF.7.A5 Ergonomischer Arbeitsplatz	• Die Arbeitsplätze werden zusammen mit der oder dem zuständigen Mitarbeitenden für Arbeitssicherheit innerhalb der FG Personal eingerichtet. • Bildschirme sollten nicht durch Unbefugte eingesehen werden können.
INF.7.A6 Aufgeräumter Arbeitsplatz	• Der Arbeitsplatz ist aufgeräumt zu hinterlassen. • Vertrauliche Informationen dürfen nicht von Unbefugten eingesehen werden können. • Beim Verlassen des Arbeitsplatzes ist der Bildschirm zu sperren.
INF.7.A7 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger	• Vertrauliche Informationen sind in den Rollcontainern und/oder den Schränken zu verschließen.

INF.8 Häuslicher Arbeitsplatz	
Beschreibung	Mitarbeitende, die das mobile Arbeiten nutzen arbeiten u.a. von ihrem häuslichen Arbeitsplatz aus. Bei einem häuslichen Arbeitsplatz kann nicht die gleiche infrastrukturelle Sicherheit vorausgesetzt werden, wie sie in den Büroräumen einer Institution anzutreffen ist. So ist z. B. der Arbeitsplatz oft auch für Besucher oder Familienangehörige zugänglich. Deshalb müssen Maßnahmen ergriffen werden, mit denen sich ein Sicherheitsniveau erreichen lässt, das mit einem Büroraum vergleichbar ist.
Anforderungen	
INF.8.A1 Sichern von dienstlichen Unterlagen am häuslichen Arbeitsplatz	• Dienstliche Unterlagen und Datenträger sind verschlossen aufzubewahren. • Es muss sichergestellt sein, dass keine dienstlichen Informationen frei zugänglich sind.
INF.8.A2 Transport von Arbeitsmaterial zum häuslichen Arbeitsplatz	• Dienstliche Unterlagen und Datenträger sind sicher zum häuslichen Arbeitsplatz zu transportieren.
INF.8.A3 Schutz vor unbefugtem Zutritt am häuslichen Arbeitsplatz	• Wenn der häusliche Arbeitsplatz nicht besetzt ist, sind Fenster zu verschließen und Türen abzuschließen. • Unbefugte dürfen keinen Zugriff auf dienstlichen Unterlagen haben.
INF.8.A4 Geeignete Einrichtung des häuslichen Arbeitsplatzes	• Der häusliche Arbeitsplatz sollte von den privaten Wohnbereichen getrennt sein. • Die genutzten Büromöbel sollten den ergonomischen Angaben entsprechen.
INF.8.A5 Entsorgung von vertraulichen Informationen am häuslichen Arbeitsplatz	• Dienstliche Unterlagen sind ausschließlich in den Räumen des Landkreises Lüchow-Dannenberg zu entsorgen, damit diese geeignet geschreddert und entsorgt werden.

INF.9 Mobiler Arbeitsplatz	
Beschreibung	Der Baustein beschreibt Sicherheitsanforderungen an mobile Arbeitsplätze (z.B. im Außendienst, auf Dienstreise etc.). Ziel ist es, für solche Arbeitsplätze eine mit einem Büroraum vergleichbare Sicherheitssituation zu schaffen.
Anforderungen	
INF.9.A1 Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes	• Kriterien zur Auswahl und Nutzung des mobilen Arbeitsplatzes sind in der „Dienstvereinbarung für das mobile Arbeiten" geregelt.
INF.9.A2 Regelungen für mobile Arbeitsplätze	• Regelungen für mobile Arbeitsplätze finden sich in der „Dienstvereinbarung für das mobile Arbeiten".
INF.9.A3 Zutritts- und Zugriffsschutz	• Wenn der mobile Arbeitsplatz verlassen wird, müssen alle dienstlichen Unterlagen und IT-Systeme für die Abwesenheit sicher verwahrt oder mitgeführt werden. Ausnahme: Wird der mobile Arbeitsplatz nur kurz verlassen, müssen die eingesetzten IT-Systeme gesperrt werden. • Es muss sichergestellt sein, dass Unbefugte keinen Zugriff auf dienstliche IT und Unterlagen haben.
INF.9.A4 Arbeiten mit fremden IT-Systemen	• Die Mitarbeitenden nutzen für die mobile Arbeit ausschließlich hauseigene IT-Systeme.
INF.9.A5 Zeitnahe Verlustmeldung	• Sollten IT-Systeme, Datenträger oder Informationen verlorengegangen sein, ist dieses umgehend an den FD 16 zu melden.
INF.9.A6 Entsorgung von vertraulichen Informationen	• Defekte Datenträger sind an den FD 16 zu übergeben. • Dienstliche Unterlagen sind ausschließlich in den Räumen des Landkreises Lüchow-Dannenberg zu entsorgen, damit diese geeignet geschreddert und entsorgt werden.
INF.9.A7 Rechtliche Rahmenbedingungen für das mobile Arbeiten	• Die Rahmenbedingungen regelt die „Dienstvereinbarung für das mobile Arbeiten". • Mit der Einzelvereinbarung, die mit jedem Mitarbeitenden, der an der mobilen Arbeit teilnehmen möchte, geschlossen wird, stimmt dieser der Dienstvereinbarung zu.
INF.9.A8 Sicherheitsrichtlinie für mobile Arbeitsplätze	• Die Sicherheitsanforderungen sind in der „Dienstvereinbarung für das mobile Arbeiten" geregelt.
INF.9.A9 Verschlüsselung tragbarer IT-Systeme und Datenträger	• Die Anmeldung an dem mobilen Arbeitsplatz erfolgt ausschließlich über die Nutzung des IGEL-Sticks. Dabei werden Benutzendenname und Passwort gefordert.
INF.9.A12 Nutzung eines Bildschirmschutzes	• Die dienstlichen Laptops sind mit einer Sichtschutzfolie ausgestattet.

INF.10 Besprechungs-, Veranstaltungs- und Schulungsraum	
Beschreibung	Besprechungs-, Veranstaltungs- und Schulungsräume zeichnen sich im Wesentlichen dadurch aus, dass sie von wechselnden Personen bzw. Personenkreisen und Besuchern und Besucherinnen in der Regel nur für einen begrenzten Zeitraum genutzt werden.
Anforderungen	
INF.10.A3 Geschlossene Fenster und Türen	• Die Fenster der Besprechungs-, Veranstaltungs- und Schulungsräume müssen beim Verlassen geschlossen werden. • Die Türen sind nach Verlassen der Räume abzuschließen.
INF.10.A4 Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen	• Die Eignung eines Raums wird geprüft bevor dieser Besprechungs-, Veranstaltung- oder Schulungsraum wird.

INF.10.A5 Fliegende Verkabelung	• Die Stromanschlüsse befinden sich in der Nähe der zu nutzenden Hardware. • Verkabelungen die über den Boden verlaufen sollten abgedeckt sein.
INF.10.A8 Erstellung eines Nutzungsnachweises für Räume	• Der Nutzungsnachweis wird über die Software zur Raumbuchung geführt.

INF.11 Allgemeines Fahrzeug	
Beschreibung	Dieser Baustein umfasst die Dienstfahrzeuge des Landkreises Lüchow-Dannenberg.
Anforderungen	
INF.11.A1 Planung und Beschaffung	• Der Einsatzzweck wird vor Beschaffung geplant. • Die Fahrzeuge verfügen über geeignete Schließsysteme. • Zum größten Teil handelt es sich um Leasing-Fahrzeuge mit einer Laufzeit zwischen einem bis drei Jahren. • In den Fahrzeugen werden keine sicherheitsrelevanten Informationen gespeichert.
INF.11.A2 Wartung, Inspektion und Updates	• Es finden regelmäßig Wartungen und Inspektionen in der Fachwerkstatt statt. • Updates werden regelmäßig eingespielt. • Reparaturarbeiten finden in der Fachwerkstatt statt. • Es werden keine IT-Komponenten verwendet, auf denen sicherheitsrelevante Informationen gespeichert, erhoben oder genutzt werden.
INF.11.A3 Regelungen für die Fahrzeugbenutzung	• Sicherheitsrelevante Unterlagen werden geschützt transportiert und nicht im Fahrzeug gelassen. • Gespräche in den Fahrzeugen werden so geführt, dass keine unbefugte Person davon Kenntnis erhält.
INF.11.A4 Erstellung einer Sicherheitsrichtlinie	• Es werden keine IT-Komponenten der Fahrzeuge genutzt, welche sicherheitsrelevante Informationen speichern oder verarbeiten.
INF.11.A5 Erstellung einer Inventarliste	• Es werden keine IT-Komponenten der Fahrzeuge genutzt, welche sicherheitsrelevante Informationen speichern oder verarbeiten.
INF.11.A6 Festlegung von Handlungsanweisungen	• Es werden keine IT-Komponenten der Fahrzeuge genutzt, welche sicherheitsrelevante Informationen speichern oder verarbeiten. • Die Fahrzeuge sind immer verschlossen, wenn sich keine befugte Person im Fahrzeug befindet. • Für Notfallsituationen wie Unfälle oder Diebstahl werden Checklisten erstellt und in den Fahrzeugen zur Dokumentation hinterlegt.
INF.11.A7 Sachgerechter Umgang mit Fahrzeugen und schützenswerten Informationen	• Die Fahrzeuge werden überwiegend verschlossen in Garagen abstellt. • Aufgrund des Platzmangels werden wenige Fahrzeuge draußen verschlossen abgestellt. • In den Fahrzeugen verbleiben bei Rückgabe keine sicherheitsrelevanten Informationen.
INF.11.A8 Schutz vor witterungsbedingten Einflüssen	• Die Fahrzeuge werden überwiegend verschlossen in Garagen abstellt. • Aufgrund des Platzmangels werden wenige Fahrzeuge draußen verschlossen abgestellt.
INF.11.A9 Sicherstellung der Versorgung	• Der Stand der benötigten Betriebsstoffe wird täglich kontrolliert und ggf. aufgefüllt. • Sollten Betriebsstoffe während der Dienstreise benötigt werden, sind diese zu beschaffen und im Anschluss mit dem Landkreis abzurechnen.
INF.11.A10 Aussonderung	• Sicherheitsrelevante Informationen verbleiben

	nicht in den Fahrzeugen. • Vor Aussonderung wird der Zustand des Fahrzeugs kontrolliert und dieses ggf. ausgeräumt.

7. Inkrafttreten

Das Informationssicherheitskonzept tritt zum 01.01.2024 in Kraft.

Freigegeben durch die Landrätin

D. Schulz

Lüchow, 06.11.2023