LOGICHECK®

IT-Sicherheitskonzept

Version 3.4, 10.11.2025

1. Einleitung

In diesem IT-Sicherheitskonzept wird die Bedeutung der Informationssicherheit für die LOGICHECK dargelegt und die grundsätzliche Informationssicherheitsstrategie beschrieben. Es ist das Ziel, die drei Grundsäulen einer sicheren Informationstechnik (Verfügbarkeit, Integrität, Vertraulichkeit) unter Berücksichtigung der wirtschaftlichen Leistungsfähigkeit des Unternehmens bestmöglich umzusetzen.

Gewährleistet werden soll:

- die Verfügbarkeit der Systeme (z. B. Schutz vor Diebstahl, Zerstörung, Ausfallzeiten, Verlust von Datenträgern),
- die Integrität der Software und der Daten (z. B. Schutz vor vorsätzlicher oder fahrlässiger Verfälschung von Programmen, Manipulation von Dateien) und
- die Vertraulichkeit von Daten (z. B. Schutz vor unbefugter Kenntnisnahme von Dateiinhalten).

Bei der Analyse der Geschäftsprozesse ist festzustellen, dass bis auf Client-PCs und Peripheriehardware (Drucker, Scanner etc.) die IT Server Infrastruktur bei einem IT-Dienstleister betrieben wird. Die Client-PCs beziehen von den Servern einzelne Datensätze zur weiteren Verarbeitung und werden auch nur auf dessen Servern gespeichert.
Da diese Daten z. T. Personenbezug enthalten, sind sie als schutzbedürftig einzustufen. Auf einer Schutzskala von „niedrig", „mittel", „hoch" ist eine Einstufung als „mittel" als angemessen anzusehen.

Anders ist das Schutzniveau der IT-Server-Infrastruktur einzuschätzen. Da sich auf den Servern auch personenbezogene Daten mit besonders schutzwürdigen Daten befinden („Personaldaten"), muss das Schutzniveau auch besonders hoch sein. Hier ist die Einhaltung von Datenschutz und -sicherheit durch verschiedene Maßnahmen (Überprüfungen, Kontrollrechte etc.) sicherzustellen. Da die Geschäftstätigkeit der LOGICHECK zudem wesentlich von der Funktionstüchtigkeit des IT-Dienstleisters abhängt, muss dieser für Notfälle gerüstet sein und dies durch geeignete Notfallpläne dokumentieren können.

Das Sicherheitsniveau der LOGICHECK bezieht sich auf alle unternehmensweit eingesetzten technischen Systeme und Verfahrensabläufe, mit deren Hilfe personenbezogene Informationen oder Informationen zu Betriebs- und Geschäftsgeheimnissen gespeichert und weiterverarbeitet werden können.

Diese Sicherheitsrichtlinie basiert auf den IT-Grundschutz-Katalogen des BSI.

2. Geltungsbereich

Diese Richtlinie gilt ohne Ausnahme verbindlich für alle Mitarbeiter für die Nutzung dienstlicher IT. Verstöße gegen die Inhalte der Richtlinie können zu arbeitsrechtlichen Konsequenzen führen.

Auch beim Abschluss von Verträgen mit externen Dienstleistern ist darauf zu achten, dass die Vorgaben dieser Richtlinie beachtet werden.

Für die Pflege und Weiterentwicklung der Richtlinie ist der Leiter der IT zuständig.

3. Bestandsanalyse

3.1 Übersicht: IT-Systeme

Nr.	Beschreibung	Grundwert	Schutzbedarf	Begründung
S1	Zentraler Anmelde Server	Vertraulichkeit	Hoch	Maximumprinzip
		Integrität	Hoch	Maximumprinzip
		Verfügbarkeit	Hoch	Maximumprinzip
		Ausgelagert, siehe IT-Sicherheitskonzept der beauftragten Firma (7.1 IT-Infrastruktur)		
S2	E-Mail-Server/ DMS System	Vertraulichkeit	Hoch	Maximumprinzip
		Integrität	Normal	Maximumprinzip
		Verfügbarkeit	Normal	Maximumprinzip
		Ausgelagert, siehe IT-Sicherheitskonzept der beauftragten Firma (7.1 IT-Infrastruktur)		
S3	Backup-Server	Vertraulichkeit	Hoch	Maximumprinzip
		Integrität	Hoch	Maximumprinzip
		Verfügbarkeit	Normal	Maximumprinzip
		Ausgelagert, siehe IT-Sicherheitskonzept der beauftragten Firma (7.1 IT-Infrastruktur)		
C1-Cx	Clients, Windows 11	Vertraulichkeit	Hoch	Über den Client kann Zugriff auf besonders sensible Daten erfolgen.
		Integrität	Normal	Die Datenhaltung erfolgt auf dem Server. Besondere Maßnahmen sind auf dem Client nicht erforderlich.
		Verfügbarkeit	Normal	Ein Ausfall kann durch andere Geräte überbrückt werden.

3.2 Übersicht: IT-Anwendungen

Nr.	Beschreibung	Personenbezogene Daten	Grundwert	Schutzbedarf	Begründung
A1	Lohnbuchhaltung	Ja	Vertraulichkeit	Hoch	Kenntnisnahme von Teilnehmerdaten durch unbefugte Dritte kann erheblichen Schaden bzw. Nachteile für Betroffene bedeuten
			Integrität	Hoch	Fehlerhafte Daten können Probleme bei der Maßnahmenabwicklung mit dem Kostenträgern und sonstigen Dritten verursachen. Auch Nachteile für Betroffene sind möglich.
			Verfügbarkeit	Hoch	Ohne Zugriff auf die Teilnehmerdaten können Aufgaben und vertragliche Pflichten des Unternehmens nicht erfüllt werden.
	Lohnbuchhaltung und Finanzbuchhaltung ist an einen Dienstleister ausgelagert, siehe Auftragsdatenverarbeitungsvertrag beauftragten Firma (7.2 Ausgelagerte Lohnbuchhaltung).				
A2	Telefonanlage	Ja	Vertraulichkeit	Hoch	
			Integrität	Hoch	
			Verfügbarkeit	Mittel	Kurzfristige Ausfälle sind hinnehmbar, Zeitweises Ausweichen auf Handy möglich.
A3	Finanzbuchhaltung	Ja	Vertraulichkeit	Hoch	Daten können dem Fernmeldegeheimnis unterliegen.
			Integrität	Mittel	
A4	Personaldatenverarbeitung		Verfügbarkeit	Niedrig	Personaldaten sind stets als besonders schützenswerte Daten einzuordnen.

Nr.	Beschreibung	Personenbezogene Daten	Grundwert	Schutzbedarf	Begründung
		Ja	Vertraulichkeit	Hoch	Daten von Maßnahmeteilnehmern können betroffen sein. Auch Betriebs- und Geschäftsgeheimnisse können betroffen sein.
			Integrität	Hoch	Anforderungen der Finanzverwaltung
	Personalakten werden im Archivraum im Tresor verschlossen.		Verfügbarkeit	Hoch	Tagesaktuelle Buchhaltung ist betrieblich erforderlich. Daten müssen auch für Kostenträger ggf. aktuell verfügbar gemacht werden können.
		Ja	Vertraulichkeit	Hoch	Dokumente enthalten besonders schützenswerte Daten
			Integrität	Hoch	
A5	Mobilfunktelefone	Ja	Vertraulichkeit	Hoch	E-Mail / Kontakte sind Besonders zu schützen. Werden per MDM privat/geschäftlicht getrennt.
			Integrität	Mittel	
			Verfügbarkeit	Mittel	
A6	Kopierer/ Mehrzweckfunktionsgerät	Ja	Vertraulichkeit	Hoch	Daten können dem Fernmeldegeheimnis unterliegen
			Integrität	Mittel	
			Verfügbarkeit	Mittel	
A7	Terminverwaltung (Outlook)	Ja	Vertraulichkeit	Hoch	Dokumente können besonders schützenswerte Daten enthalten.
			Integrität	Mittel	
			Verfügbarkeit	Hoch	
A8	E-Mail (Outlook)	Ja	Vertraulichkeit	Hoch	Die Gründe von (speziell als privat gekennzeichneten Terminen) könnten besonders schützenswerte Daten enthalten.
			Integrität	Hoch	
	Die private Nutzung von E-Mails über den Exchange-Server ist verboten. Eine Nutzung von privaten E-Mails ist nur über einen Webmailer erlaubt und das auch nur innerhalb festgelegter Pausenzeiten.		Verfügbarkeit	Niedrig	
A9	Bewerberdaten	Ja	Vertraulichkeit	Hoch	Daten können dem Fernmeldegeheimnis unterliegen
			Integrität	Hoch	
			Verfügbarkeit	Mittel	
A10	Internetseite	Ja	Vertraulichkeit	Hoch	Enthält besonders schützenswerte Daten
			Integrität	Mittel	

Nr.	Beschreibung	Personenbezogene Daten	Grundwert	Schutzbedarf	Begründung
	Eine Internetnutzung für private Zwecke ist einzig innerhalb festgelegter Pausenzeiten erlaubt.		Verfügbarkeit	Niedrig	
A11	Online-Banking	Ja	Vertraulichkeit	Mittel	
			Integrität	Mittel	
			Verfügbarkeit	Mittel	
A12	Fileserver	Ja	Vertraulichkeit	Hoch	
			Integrität	Hoch	
			Verfügbarkeit	Mittel	Werden versioniert / mehrfach vorgehalten.
A15	IT-Wartung	Ja	Vertraulichkeit	Mittel	
			Integrität	Mittel	
			Verfügbarkeit	Hoch	

Ausgelagert, siehe IT-Sicherheitskonzept der beauftragten Firma (7.1 IT-Infrastruktur).

4. Schwachstellen-/Risikoanalyse

Da die Geschäftstätigkeit der LOGICHECK wesentlich von der Funktionstüchtigkeit des IT-Dienstleisters abhängt, muss dieser für Notfälle gerüstet sein und dies durch geeignete Notfallpläne dokumentieren können. Siehe hierzu Punkt 12.1.

5. Umgang mit Informationen

Für Geschäftsprozesse, Informationen, Anwendungen und IT-Systeme werden Verantwortliche („Eigentümer“) festgelegt.
Informationen sind anhand ihres Schutzbedarfs klassifiziert. Die folgenden Schutzbedarfskategorien sind vorgegeben:

- Normale Information (kein spezieller Schutz; keine Zustimmung erforderlich)
- Vertrauliche Information (optionaler Schutz; sollte nur zwischen den jeweiligen Parteien ausgetauscht werden)
- Persönliche Information (Schutz erforderlich; benötigt Zustimmung des Absenders bei Weiterleitung)

Ziel ist es, Informationen entsprechend ihrem Schutzbedarf zu verarbeiten. Nur wenn IT-Benutzer und Verantwortliche wissen, welche Informationen besonders schutzbedürftig sind, können sie diese auch angemessen schützen. Aus dem Schutzbedarf der Informationen leitet sich letztendlich der Schutzbedarf der IT-Systeme ab, auf denen die Informationen verarbeitet werden.
Die Verantwortlichen legen fest, wer unter welchen Bedingungen auf Informationen zugreifen bzw. Anwendungen und IT-Systeme nutzen darf.

6. Rechtsvorschriften

Beim Einsatz der IT sind Gesetze, Vorschriften und (interne) Regelungen einzuhalten, insbesondere:

- Bundesdatenschutzgesetz (BDSG)
- Jugendschutz-Gesetz (JuSchG)
- Urheberrechts-Gesetz (UrhG)
- Strafgesetzbuch (StGB)
- Telemediengesetz (TMG) und Telekommunikationsgesetz (TKG).

Logicheck hat einen Datenschutzbeauftragten bestellt, der Logicheck in allen Datenschutzbelangen und

hinsichtlich der Einhaltung der Datenschutzvorschriften, insbesondere bei der Umsetzung und Einhaltung der technischen und organisatorischen Maßnahmen zum Datenschutz nach i.S.d. Art. 32 DSGVO, berät, deren Einhaltung prüft.

7. Organisation

7.1 IT-Infrastruktur

Bis auf Client-PCs und Peripheriehardware (Drucker, Scanner etc.) befindet sich die Server IT-Infrastruktur bei folgendem IT-Dienstleister:

Jerocom GmbH
Löhdorfer Str. 281
42699 Solingen

Dieser stellt der Firma Logicheck Ressourcen für die Nutzung eigener virtueller Server zur Verfügung.
Alle datenschutzrelevanten Prozesse und Maßnahmen zur Einhaltung der Datensicherheit werden in folgenden Unterlagen beschreiben:

- Ein IT-Sicherheitskonzept des IT-Dienstleisters
- Einen Desaster Recovery Plan des IT-Dienstleisters

7.2 Ausgelagerte Lohnbuchhaltung

Die komplette Finanz- und Lohnbuchhaltung ist an folgendes Steuerbüro ausgelagert:
Görgen & Partner, Philipp-Reis-Str. 15, 55469 Simmern.
Alle datenschutzrelevanten Prozesse und Maßnahmen zur Einhaltung der Datensicherheit werden in einem separaten Auftragsdatenverarbeitungsvertrag („ADV-Vertrag“) nach §11 BDSG beschrieben.

7.3 Stellen

Die unternehmensweiten IT-Dienste sind durch den IT-Leiter zu administrieren und zu war-ten. Wenn Projektziele den Sicherheitsanforderungen entgegenstehen, obliegt der Unternehmensleitung die Entscheidung, welche Anforderungen eine höhere Priorität haben. Diese muss evtl. bestehende Bedenken seitens des IT-Leiters stets angemessen berücksichtigen.
Der IT-Leiter hat dafür zu sorgen, dass Sicherheitslücken frühzeitig geschlossen werden. Zu diesem Zweck hat er sich stets auf den neuesten Wissensstand zu bringen und die IT-Benutzer in Sicherheitsfragen zu unterstützen und zu beraten.

7.4 Schulung und Sensibilisierung

IT-Benutzer sind vom IT-Leiter vor der erstmaligen Nutzung der jeweiligen IT-Dienste zu schulen.
Schulungsinhalte sind:

- Handhabung der jeweilig verwendeten IT-Dienste
- Inhalte der Sicherheitsleitlinie und der Sicherheitsrichtlinien zu verschiedenen Themen (Notfallvorsorge, Datensicherung etc.) sowie die umzusetzenden Sicherheitsmaßnahmen
- Sensibilisierungsmaßnahmen („Warum ist Informationssicherheit so wichtig für mich und meinen Arbeitgeber?“)
- Rechtliche Rahmenbedingungen

Darüber hinaus schult der Datenschutzbeauftragte Mitarbeiter im Hinblick auf datenschutz-rechtlich relevante Aspekte.

7.5 Vertretungsregeln

Für den Fall der Abwesenheit (Dienstreise, Urlaub, Krankheit) sind Vertreter zu benennen, die vom Stelleninhaber einzuweisen und zu informieren sind.

7.6 Datenschutz

Zur Absicherung allgemeiner organisatorischer Maßnahmen zur Datensicherheit wird bei Logicheck eine Datensicherheitsrichtlinie eingesetzt, die von allen Mitarbeitern einzuhalten ist. Die Datensicherheitsrichtlinie ist in einem separaten Dokument geregelt.
Für die LOGICHECK ist folgende Person als Datenschutzbeauftragte bestellt:

Claudia Bischof
datenschutz@logicheck.de

8. Verwaltung und Nutzung von IT-Diensten

8.1 Allgemeines

Die E-Mail- und Internet-Programme sowie die Hardwarekomponenten werden durch den IT-Leiter konfiguriert und gewartet. Art und Umfang der Maßnahmen erfolgen in Absprache mit dem IT-Leiter und richten sich nach dem als „mittel" angesehenen IT-Sicherheitsniveau von LOGICHECK. Änderungen an den Sicherheitseinstellungen durch die IT-Benutzer sind nicht gestattet.

8.2 Sicherheitsupdates

Die IT-Systeme werden durch ein Patch Management System (Microsoft Intune) auf dem aktuellen Stand gehalten. Windows Updates und „Third Party Applikation" werden in Wellen (Max. 10 Tage nach Release) erzwungen auf allen Systemen installiert.
Dies beinhaltet auch Treiber/Bios Versionen der verwendeten Hardware.

8.3 Beschaffung

Für die Beschaffung von Soft- und Hardware wird als Grundlage ein Anforderungsprofil er-stellt, das neben fachlichen und technischen Ausstattungsmerkmalen sowie ergonomischen Aspekten auch Anforderungen an die Informationssicherheit sowie die Integration in vorhandene oder geplante, informationstechnische Infrastruktur beschreibt. Die Beschaffung folgt darüber hinaus den für den jeweiligen Bereich geltenden Normen (ISO, DIN).
Hard- und Software werden in einer Inventardatenbank erfasst und regelmäßig aktualisiert. Diese Datenbank wird vom IT-Leiter geführt.
Es sind im Rahmen der Kommunikation und Archivierung bevorzugt Programme zu beschaffen, die eine Verschlüsselung ermöglichen.

8.4 Einsatz

Die IT-Dienste sind von Mitarbeitern nur für betriebliche Belange aufgrund der festgelegten Aufgaben oder aufgrund einer Weisung der Geschäftsleitung zu nutzen.
Dienste und Berechtigungen, die nicht oder nicht mehr benötigt werden, sind auf Geheiß des IT-Leiters mit/durch den IT-Dienstleister zu deaktivieren.
Der IT-Leiter hat in regelmäßigen Abständen zu kontrollieren, dass die Berechtigungen noch aktuell sind und stets aufs notwendige Maß beschränkt sind. Entsprechend nötige Anpassungen sind unverzüglich von ihm umzusetzen.
Soft- und Hardware sind analog zu Abschnitt 8.1. Allgemeines in Absprache mit dem IT-Leiter zu konfigurieren, dass ohne weiteres Zutun der IT-Benutzer optimale Sicherheit erreicht werden kann. Default-Einstellungen sind zu überprüfen und Default-Passwörter zu ändern.
Es sind angemessene Sicherheitsprodukte einzusetzen. Die Wahl trifft der IT-Leiter, nach angemessener

Berücksichtigung der Empfehlungen des IT-Dienstleisters.

8.5 Wartung

Die mit Pflege und Wartung verbundenen Maßnahmen sind vom IT-Leiter nach Art, Inhalt und Zeitpunkt zu protokollieren.
Der Zugriff auf Daten durch Wartungstechniker ist soweit wie möglich zu vermeiden. Die eingeräumten Zutritts-, Zugangs- und Zugriffsrechte sind auf das notwendige Minimum zu beschränken und nach den Arbeiten zu widerrufen bzw. zu löschen. Bei Arbeiten an organi-sationsweiten IT-Diensten mit sensiblen Informationen ist das Vier-Augen-Prinzip anzuwenden.
Falls LOGICHECK-Mitarbeiter durch Arbeiten am IT-System von der Ausübung ihrer Arbeit teilweise oder gar gänzlich abgehalten werden könnten, müssen die Systemarbeiten, wann immer möglich außerhalb der normalen LOGICHECK-Arbeitszeiten stattfinden.
Im Anschluss an die Wartungs- oder Reparaturarbeiten ist die ordnungsgemäße Funktion der gewarteten IT-Systeme durch den IT-Leiter zu überprüfen und zu dokumentieren.

8.6 Schutz gegen Computer-Viren

Auf allen Computern wird lokal ein Virenscanner installiert, der eine lokale Firewall beinhaltet.
Gleichzeitig wird die Kommunikation mit externen Netzen durch eine externe Firewall kon-trolliert. Ein- und ausgehende E-Mails werden mit einem Spam-Filter mit Antivirenprogramm auf Computer-Viren sowie Malware geprüft. Weitere IT-Kommunikation wird mit einem Proxy mit Antivirenprogramm überwacht. Es gibt ein Verfahren, welches bei Feststellung eines Virus angewandt wird (siehe Punkt 12.2 Verhalten bei Feststellung eines Virus).
Innerhalb der Default-Einstellungen ist sicherzustellen, dass Datei-Endungen nicht unter-drückt werden. Andernfalls wird es dem Nutzer erschwert, Dateiarten zu unterscheiden und Gefährdungspotenziale einzuschätzen.

8.7 Internet-Browser und E-Mail-Client

Die Mitarbeiter sind angewiesen, dass …

- bei Nutzung des Browser-Cache dieser regelmäßig (nach der Sitzung) zu löschen ist.
- die Funktion des Browsers, heruntergeladene Dateien automatisch zu öffnen, zu de-aktivieren ist. Aktive Inhalte dürfen bei der Anzeige in E-Mail-Clients nicht automatisch ausgeführt werden (Vorschaufunktion deaktivieren).
- von der Funktion automatischer Lesebestätigungen abzusehen ist, um Spamversen-der nicht unnötig zu unterstützen.
- bei einer automatischen Weiterleitung von E-Mails die Vertraulichkeit zu wahren ist. Der Mitarbeiter hat sich zu vergewissern, dass alle Empfänger die E-Mails auch lesen dürfen.
- die Funktion des Browsers zu deaktivieren ist, die das automatische Ausfüllen von Formularen auf Internetseiten durch abgespeicherte persönliche Informationen oder Passwörter ermöglicht.
- bei besonderen Vorkommnissen (z. B. Verdacht auf Viren, Zugriffsversuchen von Hackern) erste Notmaßnahmen entsprechend dem geschilderten Vorgehen in Punkt 12.2 Verhalten bei Feststellung eines Virus selbst getroffen werden. Die IT ist unverzüglich zu informieren.
- der installierte Virenscanner nicht deaktiviert wird und Updates auf schnellstem Wege installiert werden
- bei der generellen Kommunikation im Internet (E-Mail, Chat-Rooms, Social Networks) auf eine repräsentative Darstellung im Sinne des Unternehmens Rücksicht genommen wird
- vertrauliche Informationen (ob geschäftlich oder privat) dementsprechend behandelt werden und nicht unbedacht an Dritte weitergegeben werden
- nur dann im Namen des Unternehmens gesprochen werden darf, wenn dies ausdrücklich erlaubt wird.

Die Mitarbeiter werden vom IT-Leiter in diesen Angelegenheiten regelmäßig unterrichtet.

8.8 Sicherheitsgateway (Firewall)

Nur mit einer geeigneten Firewall kann der Anschluss an ein externes Netz erfolgen. Die Firewall ist so konfiguriert und administriert, dass sie einen effektiven Schutz darstellt und Manipulationen verhindert werden. Dieses wird durch Perimeterschutz, Spamfilter und Proxy garantiert.
Wie in Punkt 8.6 Schutz gegen Computer-Viren angeführt, wird ein doppelter Schutz gewährleistet. Zum einen

schützt eine lokale Firewall – kombiniert mit einem Virenscanner – jeden einzelnen Computer und zum anderen wird der Zugriff nach außen durch eine externe Firewall geschützt.
Aktive Inhalte sind zentral an der Firewall oder am Proxy zu filtern.
Bei der Firewall sind die Filterregeln restriktiv zu wählen („alles, was nicht erlaubt ist, ist verboten"). Die IT-Benutzer dürfen jedoch nicht durch eine Vielzahl von Meldungen belästigt und in ihrer Arbeit beeinträchtigt werden. Alle weiteren Komponenten, die der Kommunikation zwischen geschützten internen und ungeschützten externen Netz dienen, müssen sicher angeordnet werden.
Computer dürfen nur mit dem Internet verbunden werden, wenn sie mit einer Personal Fire-wall ausgestattet sind.

8.9 Revision

Alle Maßnahmen an IT-Diensten sind zu dokumentieren. Tätigkeiten des IT-Dienstleisters sind zu protokollieren. Es ist eine regelmäßige Kontrolle der Funktionalität der IT-Dienste, der Informationssicherheit und der Einhaltung der Richtlinien von dem IT-Leiter erforderlich. Sicherheitsrelevante Ereignisse und Zugriffe auf kritische Bereiche sind automatisch zu protokollieren und durch Administratoren regelmäßig zu überprüfen. Bei der Protokollierung sind Datenschutzaspekte zu beachten.

8.10 Weitergaberegelungen

Bei der Weitergabe von Informationen ist ihr Schutzbedarf zu beachten und eine geeignete Versandart zu wählen. Vertrauliche Informationen oder Datenträger (CD-ROM, DVD, Festplatte, USB-Sticks etc.) mit vertraulichen Informationen dürfen erst dann versendet werden, wenn die Vertraulichkeit beim Versand gewährleistet ist. Der Empfänger der Informationen ist zur vertraulichen Behandlung zu verpflichten.
Wird Hardware außer Haus gegeben, sind, sofern dies möglich ist, alle vertraulichen Informationen, die sich in Datenspeichern befinden, vorher sicher zu löschen. Ist dies nicht möglich, so ist der Vertragspartner auf Geheimhaltung zu verpflichten. Die Übergabe bzw. der Transport ist sicher zu gestalten.

8.11 Entsorgung

Belege und Druckausgaben, die vertrauliche Informationen beinhalten, müssen getrennt vom übrigen Abfall durch LOGICHECK-Mitarbeiter entsorgt werden. Hierfür stehen Shredder mit einer Sicherheitsstufe von mindestens Sicherheitsstufe P-4 (DIN 66399) bereit. Elektronische Datenträger mit vertraulichen Informationen, die nicht weiter benötigt werden, sind vor der Entsorgung sicher zu löschen. Eine fachgerechte Entsorgung erfolgt bei zerstörten Datenträgern über den IT-Dienstleister

9. Zutritt und Zugang

Zugangsregelungen und vergebene Berechtigungen zu den LOGICHECK-Büros und dem Archiv; diese werden vom IT-Leiter sorgfältig in einer zentralen Liste derart dokumentiert, dass jederzeit sichtbar wird, welche Person zu welchen Systemen und Diensten Zugang hat bzw. früher hatte.
Diese Zugangsberechtigungen werden vom IT-Leiter auf Aktualität und Notwendigkeit in regelmäßigen Abständen überprüft.
Das Ausprobieren von weiteren Diensten und Zugriffsrechten als den explizit Erlaubten ist verboten.

9.1 Allgemeine Zutritts- und Zugangsregelungen

Der Arbeitsplatz ist so zu hinterlassen, dass Unbefugte keinen Zugriff auf vertrauliche Informationen und IT-Anwendungen ermöglicht wird. Hierzu sind Räume falls möglich zu ver-schließen. Bei nicht verschließbaren Räumen sind die vertraulichen Informationen in verschlossenen Schränken aufzubewahren. IT-Geräte sind zum Schutz von unbefugten Personen mit einer passwortgeschützten Desktopsperre ausgestattet. Dieser muss bei Verlassen des Arbeitsplatzrechners manuell oder automatisch aktiviert werden.
Alle Notebooks sind grundsätzlich zu verschlüsseln. Der Zugriff auf Notebooks und Computer wird verbindlich über Windows Active Directory und entsprechende Berechtigungen gesteuert. Zusätzlich sind die Festplatten standardmäßig mit einer Verschlüsselungssoftware zu schützen.
In Bereichen mit Publikumsverkehr sind Monitore, Drucker und Faxgeräte so aufzustellen, dass das Risiko der Einsichtnahme Dritter möglichst ausgeschlossen wird.

Zum Zugang zu den Kommunikationsdiensten hat jeder User eine eigene ID sowie ein vorgegebenes Passwort erhalten. Dieses ist entsprechend den Passwort-Regeln (siehe 9.2 Pass-wort-Regeln) zu ändern und streng vertraulich zu behandeln. Für die Sicherung vor Verlust sowie vor Preisgabe an Dritte sind Vorkehrungen zu treffen.
Wenn der Verdacht besteht, dass die eigenen Zugangs- und Zugriffsberechtigungen unberechtigt durch Dritte genutzt werden, ist das Passwort umgehend zu ändern und die IT um Rat zu fragen.

9.2 Passwort-Regeln

Folgende Regeln sind zu beachten:

- Passwörter sind nirgends zu notieren und niemandem mitzuteilen.
- Das Passwort darf nur dem Benutzer bekannt sein.
- Passwörter müssen eine Mindestlänge von 12 Zeichen haben. Das Passwort ist aus 3 von 4 folgenden Kategorien zu gestalten: Großbuchstaben, Kleinbuchstaben, Zahlen und Spezialzeichen.
- Passwörter dürfen nicht leicht zu erraten sein. Vor- und Familiennamen oder Geburtstage sind beispielsweise nicht zur Bildung von Passwörtern geeignet. Es dürfen niemals Trivialpasswörter verwendet werden (z. B. 4711; 12345 oder andere nebeneinanderliegende Tasten).
- Die Passwörter sind spätestens alle 120 Tage zu wechseln.
- Einmal genutzte Passwörter sind nicht wieder zu verwenden. Dabei ist zu beachten, dass, die letzten 4 Passwörter nicht mehr zu wählen sind und mindestens ein Tag vor dem erneuten Ändern eines Passworts liegen muss.
- Benutzer haben den Empfang von Initial-Passwörtern immer zu bestätigen und müssen diese sofort wechseln.
- Alle IT-Systeme sind zum Schutz vor unbefugten Personen mit einer passwortunter-stützten Desktopsperre ausgestattet, diese ist auch immer zu benutzen.
- Sofern möglich, soll Windows Hello for Business aktiviert werden, um eine weitere sichere Stufe der Authentifizierung zu ergänzen.

9.3 Schutz von sensiblen Räumen

Mit Ausnahme des Archivraums befinden sich datenschutztechnisch besonders sensible Räume lediglich beim IT-Dienstleister und nicht beim Unternehmen selbst.
Der Archivraum selbst ist abgeschlossen, alarm- und kameragesichert und besonders schützenswerte Dokumente (wie z. B. Personalakten) werden zudem in einem eingebauten Tresor eingelagert.

9.4 Besonderheiten Home-Office

Bei Tätigkeiten im Rahmen der Home-Office Regelung muss der Mitarbeiter sicherstellen, dass der Raum, in dem er seine Arbeit verrichtet, jederzeit abgeschlossen werden kann und weder Familienmitglieder noch Bekannte Zugriff auf die betrieblichen Daten von LOGICHECK haben. Hierzu wurden ergänzende Vereinbarungen zum Arbeitsvertrag mit den Mitarbeitern geschlossen.

9.5 Besucherregelung

Besucher werden am Eingang abgeholt und in eine Besucherliste mit Namen, Datum, Start- und Endzeit des Besuchs eingetragen. Nach Verlassen der Räumlichkeiten müssen die Besucher ihren Besuch quittieren/unterschreiben. Besucher sind stets in Begleitung eines Ange-stellten und ihnen wird dabei kein Einblick in unbefugte Systeme und Daten gestattet.

10. Regelungen für spezifische IT-Dienste

10.1 Kommunikationsspezifische Regelungen

Beim Datenaustausch ist eine geeignete Versandart zu nutzen. Die Vertraulichkeit ist beim Versand zu gewährleisten:

- Geschäftliche E-Mails sind nicht auf eine allgemeine E-Mail-Adresse umzuleiten.
- Es sind keine vertraulichen Nachrichten auf Anrufbeantworter zu sprechen.
- Die vom Faxgerät auf der Gegenseite vor dem eigentlichen Sendevorgang abgegebene Kennung ist sofort zu überprüfen, damit bei eventuellen Wählfehlern die Übertragung unverzüglich abgebrochen werden kann.
- Beim Faxversand schutzbedürftiger Dokumente ist ein Sendezeitpunkt mit der Gegenseite abzustimmen, damit diese das Fax sofort entgegennehmen kann.
- Ausdrucke mit vertraulichen Informationen sind umgehend aus dem Drucker zu entfernen.

10.2 Fernzugriff auf das interne Netz

Eine externe Anbindung an das interne Netz ist speziell zu regeln. Sofern möglich, ist der Fernzugriff (z.B. durch VPN) auf notwendige Netze zu beschränken. Der Fernzugriff ist sicher zu konfigurieren. Für besonders sensible Bereiche ist entweder ein Fernzugriff auszuschließen oder auf Not-fälle zu beschränken. Der Notfall und die Verfahrensweise während des Notfalls sind genau zu definieren.

10.3 Zugriff auf das Mail-System

10.3.1 Zugriff durch mobile Geräte

Der Zugriff auf das Mail-System wird mithilfe von Reverse Proxy realisiert. Die Anmeldung erfolgt mit E-Mail-Adresse, Benutzernamen und einem gewählten Passwort. Zusätzlich ist die Anmeldung durch eine Zwei-Faktor-Authentifizierung (2FA) zu bestätigen.
Dabei muss folgende Richtlinie beachtet werden:

- IT-Leiter hat den Benutzer für Webmail Nutzung freigegeben.
- Die mobilen Geräte müssen Microsoft EAS (Exchange Active Sync) unterstützen
- Kennwort-Schutz auf mobilem Endgerät ist aktiv.
- Updates müssen aktiviert werden und stündlich abgerufen werden

Für die Eingabe des Passworts können bis zu 4 Fehlversuche getätigt werden, bevor der Benutzer gesperrt wird.

11. Notfallvorsorge

11.1 Datenverfügbarkeit

Um die Verfügbarkeit zu gewährleisten, ist durch den IT-Dienstleister Folgendes sicherzustellen:

- Daten sind durch Katalogisierung so aufzubewahren, dass sie problemlos wiedergefunden werden können.
- Um das Risiko eines Datenverlusts zu reduzieren, werden regelmäßig Datensicherungen durchgeführt

  Um eine konstante Datenverfügbarkeit zu gewährleisten, werden die Daten redundant auf den Servern gespeichert. Die Ausfallsicherheit wird durch Spiegelung der Systeme und redundante Datenhaltung garantiert.

12. Verhalten bei Sicherheitsvorfällen

Die folgenden Verhaltensregeln sind bei den verschiedenen Sicherheitsvorfällen einzuhalten:
Sobald ein Fehler oder ein anderes Problem auftritt, ist umgehend die Geschäftsführung zu benachrichtigen. Im Umgang mit Sicherheitsvorfällen sind Ehrlichkeit und Kooperationsbereitschaft besonders wichtig. Die Meldung von Sicherheitsvorfällen wird daher immer positiv gewertet!
Die Anweisungen des IT-Leiters sind zu befolgen.

12.1 IT-Notfallplan

Da alle wichtigen IT-Systeme an einen IT-Dienstleister ausgelagert sind, ist ein IT-Notfallplan für LOGICHECK derzeit noch nicht notwendig; im Katastrophenfall könnte der Betrieb mit geringem Aufwand zeitnah in beliebigen anderen Büroräumen mithilfe des IT-Dienstleisters fortgeführt werden.

12.2 Verhalten bei Feststellung eines Virus

Die Computer werden grundsätzlich von einem Anti-Virenscanner überwacht und dabei wer-den die Viren automatisch vom befallenen Computer unschädlich gemacht. Über jedes Ereignis, wenn ein Virus auftritt, wird die IT-Leitung umgehend per E-Mail informiert.
Für den Fall, dass ein Virus trotzdem nicht automatisch unschädlich gemacht werden kann, hat der Mitarbeiter unverzüglich das LAN-Kabel zu ziehen und die IT-Leitung über diesen Vorfall zu informieren, diese Verfahren wird Teilweise Proaktiv Automatisch von Microsoft Defender durchgeführt und das Gerät muss durch den IT-Leiter wieder freigeben werden.
Mit der IT-Leitung wird auch das weitere Vorgehen zur Beseitigung des Virus besprochen. Mögliche Ursachen für die Entstehung und Verbreitung müssen festgehalten werden.

12.3 Verlust von Hardware

Der Verlust von Hardware ist direkt dem IT-Leiter zu melden. Sofort vorzunehmen sind eine Passwortänderung und eine Sperrung der SIM-Karte. Bei Verlust von mobilen Geräten (z. B. iPhone, Android) ist es möglich, diese per Software fernzulöschen (beim iPhone z. B. über Exchange).

13. Evaluierung und Anpassung dieses IT-Sicherheitskonzeptes

Das Sicherheitskonzept ist bei jeder Änderung der aktuellen und personellen Gegebenheiten und aus sonstigen Anlässen, die Auswirkungen auf das Sicherheitskonzept haben, fortzuschreiben und spätestens nach einem Jahr zu überprüfen.

Ausgefüllt für die Organisation von
Marcel Junk, Leiter IT
T 06721 – 6840 214
E m.junk@logicheck.de

Gültigkeitsbereich

LOGICHECK Prüfprozesse und SaaS-Dienste GmbH
Stromberger Str. 47b
55411 Bingen am Rhein

LOGICHECK Schadenmanagement Öl/Umwelt GmbH
Rheinpromenade 6
40789 Monheim am Rhein