



ESH
Essener Systemhaus

Dienstleisterrichtlinie

zur Nutzung der IT-Infrastruktur des Essener Systemhauses

Themenbereich	ISMS
Klassifizierung	Intern
Status	Freigegeben
Eigentümer	Stabsstelle ISMS
Version	2.2
Datum	14.10.2025

INHALTSVERZEICHNIS

Abkürzungsverzeichnis.....	II
Änderungshistorie und Freigabe.....	II
Mitgeltende Dokumente.....	II
1 Einleitung.....	1
2 Geltungsbereich des Dokuments.....	1
3 Zielsetzung.....	2
4 Verbindliche Regeln für alle Dienstleistungsmitarbeiter*innen	2
4.1 Grundregeln für alle Dienstleistungsmitarbeiter*innen.....	2
4.1.1 Allgemeines.....	2
4.1.2 Zutritt.....	3
4.1.3 Umgang mit Daten und Informationen.....	3
4.1.4 Passwörter und Berechtigungen.....	3
4.1.5 Hard- und Software.....	4
4.1.6 Einsatz von Fremdhardware und Fremdsoftware	4
4.1.7 E-Mail, Internet und Telekommunikation.....	4
4.1.8 Sicherheitsvorfälle.....	4
5 Authentisierung.....	5
5.1 Kennwortalter und Kennwortkomplexität.....	5
6 Klassifizierung von Daten und Informationen	5
7 Verhalten bei Unregelmäßigkeiten	6
8 Datenschutz.....	6
9 Beendigung des Dienstleistungsverhältnisses.....	6
10 Sanktionen	7

ABKÜRZUNGSVERZEICHNIS

ESH	Essener Systemhaus
IT	Informationstechnologie
ISMS	Informationssicherheitsmanagementsystem
OTP	One-Time Password

ÄNDERUNGSHISTORIE UND FREIGABE

Änderungen					
Name	Version	Datum	Beschreibung	Freigabe am	Freigabe durch
Blaß	0.1	28.08.2018	Erster Entwurf		
Rauprich	0.2	05.10.2018	Überarbeitung Entwurf		
Blaß	1.0	19.11.2018	Erste Version		
Nehmer	1.1	10.02.2021	Anpassung Passwortsafe		
Nehmer	1.2	24.03.2022	Review – Anpassung Dokumentenvorlage & Klassifizierung	25.03.2022	H.U. Rauprich
Nehmer	2.0	18.04.2023	Review Anpassung Fremdhardware, neue Kennwortrichtlinie	18.04.2023	H.U. Rauprich
C. Nehmer	2.1	12.04.2024	Review Ergänzung Kap. 5.1 Passphrase		
C. Nehmer	2.2	14.10.2025	Review Keine Änderungen		

MITGELTENDE DOKUMENTE

1 EINLEITUNG

Das Essener Systemhaus (im Folgenden ESH genannt) ist als zentraler Dienstleister für die Stadtverwaltung Essen und deren Beteiligungen maßgeblich auf eine funktionierende IT-Infrastruktur angewiesen. Die IT-Systeme, Anwendungen und Daten bilden das Rückgrat der Arbeitsprozesse, die störungsfrei und zuverlässig zur Verfügung gestellt werden müssen.

Durch die Gewährung eines Zugangs zur IT-Infrastruktur entstehen IT-Risiken, die nur durch eindeutige Vorgaben sowie deren Einhaltung reduziert werden können. Die Betriebsleitung des ESH ist sich der Gefahren, als auch der nötigen Mitwirkung der jeweiligen Dienstleister, bewusst. Aus diesem Grunde wird die vorliegende Richtlinie erlassen.

Durch die persönliche Unterschrift bestätigt die/der jeweilige Dienstleistende den Empfang sowie die strikte Einhaltung dieser Richtlinie.

Alle Dienstleistenden verpflichten sich hiermit, die nachfolgenden Grundsätze, Regeln und Maßnahmen durch ihr aktives Tun mit Leben zu füllen und die Weiterentwicklung der Informationssicherheit aktiv zu unterstützen. Verbesserungen und Anregungen zu dieser Richtlinie richten Sie bitte an ihre*n jeweiligen Ansprechpartner*in, oder aber an die Stabsstelle ISMS (Email: informationssicherheit@esh.essen.de).

2 GELTUNGSBEREICH DES DOKUMENTS

Dieses Dokument gilt für externe Beschäftigte, die Zugang zur Infrastruktur des ESH erhalten, unabhängig ob diese durch das ESH oder einen ESH Kunden beauftragt wurden.

3 ZIELSETZUNG

Das ESH setzt zur Absicherung der eigenen IT-Infrastruktur verbindliche Standards. Diese Standards dienen zur Erreichung folgender Sicherheitsziele:

- eine angemessen hohe Informationssicherheit für das ESH und die Auftraggeber des ESHs,
- die Sicherstellung der
 - Vertraulichkeit,
 - Authentizität
 - Integrität sowie
 - Verfügbarkeitfür die in den Geschäftsprozessen genutzten Daten, Informationen und IT-Systeme,
- die Nachvollziehbarkeit des Zutritts, Zugangs und Zugriffs zu den IT-Systemen und Informationen sowie aller sicherheitsrelevanten Vorgänge gemäß den gesetzlichen Vorgaben,
- die Erfüllung der rechtlichen Vorgaben und vertraglichen Vereinbarungen.

Neben technischen Maßnahmen hat die Betriebsleitung des ESHs die Stabsstelle ISMS eingerichtet, um ein Informationssicherheitsmanagement zu betreiben. Das Ziel des Informationssicherheitsmanagements ist, die technischen und organisatorischen Sicherheitsmaßnahmen sowie die notwendigen Sicherheitsprozesse für das ESH optimal und wirkungsvoll zu gestalten. Die Stabsstelle ISMS ist der zentrale Ansprechpartner zu allen Informationssicherheitsfragen.

4 VERBINDLICHE REGELN FÜR ALLE DIENSTLEISTUNGSMITARBEITER*INNEN

Ein sicherheitsgerechtes Verhalten aller Nutzer*innen sowie der im Hause bzw. im Netzwerk oder an IT-Einrichtungen des ESH oder ihrer Kunden tätigen Dienstleistungsmitarbeiter*innen ist zur Erreichung der Sicherheitsziele zwingend erforderlich. Daher werden die nachstehenden Grundregeln zur Informationssicherheit für alle Dienstleistungsmitarbeiter*innen aufgestellt und sind hiermit für diese verbindlich.

Die/der jeweilige Dienstleistungsmitarbeiter*in bestätigt durch die Unterschrift der angefügten Erklärung die Kenntnisnahme und Einhaltung dieser Dienstleisterrichtlinie. Die unterschriebene Erklärung wird zurück an die/den jeweilige*n Ansprechpartner*in des ESH gesendet. Nach Eingang wird der Zugang freigegeben.

4.1 GRUNDREGELN FÜR ALLE DIENSTLEISTUNGSMITARBEITER*INNEN

Für alle Dienstleistungsmitarbeiter*innen ergeben sich die folgenden Regeln im Umgang mit Unternehmensdaten und IT-Einrichtungen des ESH oder seiner Kunden. Diese dienen sowohl dem Schutz des Betriebes und seiner Mitarbeiter*innen als auch der einzelnen Dienstleistungsmitarbeiter*innen:

4.1.1 ALLGEMEINES

- Jede*r einzelne Dienstleistungsmitarbeiter*in ist im Rahmen ihrer/seiner Tätigkeit für die Erreichung und Einhaltung der Informationssicherheit zuständig und im Rahmen ihrer/seiner Möglichkeiten für die Unternehmensdaten und –systeme des ESH mit verantwortlich.
- Die Einhaltung der Informationssicherheitsregelungen ist als wichtiger Bestandteil einer jeden Dienstleistungstätigkeit zu verstehen und zu akzeptieren. Ein damit einhergehender Mehraufwand ist im Sinne des Unternehmens und seiner Mitarbeiter*innen.

Sicherheit geht vor Bequemlichkeit!

- Die gesetzlichen Anforderungen sind einzuhalten. Beispielhaft werden EU-DSGVO, BDSG, LDSG NRW und Strafgesetzbuch genannt. Die/der Dienstleister*in hat sich vor der Tätigkeit über die jeweils auf ihn wirkenden Gesetze zu informieren.
- Bei Audio-, Video- und Programmdateien ist in jedem Fall das Urheberrecht zu beachten.

4.1.2 ZUTRITT

- Dienstleistungsmitarbeiter*innen dürfen sich nur in Begleitung und unter Aufsicht von Mitarbeitern*innen des ESH in den nicht-öffentlichen Räumlichkeiten des ESH bewegen. Sie müssen sich an der Türsprechstelle melden und werden dort von den besuchten Mitarbeiter*innen abgeholt bzw. wieder zum Ausgang zurückbegleitet.
- Dienstleistungsmitarbeiter*innen erhalten bei wiederkehrenden Tätigkeiten ein Identifikationsmittel zur Zutrittssteuerung. Dieses ist vor Beschädigung oder Verlust zu schützen. Jeder Verlust ist unverzüglich der*m jeweiligen Ansprechpartner*in zu melden.
- Die Türen zu und zwischen den unterschiedlichen Sicherheitsbereichen sind grundsätzlich geschlossen zu halten.
- Bei Abwesenheit sind ggf. noch laufende IT-Systeme gegen unberechtigten Zugriff zu sperren.

4.1.3 UMGANG MIT DATEN UND INFORMATIONEN

- Alle Daten und Dokumente sind klassifiziert (öffentlich, intern, vertraulich, streng vertraulich) und müssen entsprechend behandelt werden. Somit dürfen Dokumente nur an den jeweils berechtigten Personenkreis weitergegeben werden.
- Bestehen im Einzelfall Zweifel an der Berechtigung einer Person (auch bei Vertragspartnern), so ist zuvor durch den jeweiligen Auftraggeber eine Klärung herbeizuführen.
- Sollten Zweifel nicht ausgeräumt werden können, muss die/der Informationssicherheitsbeauftragte hinzugezogen werden.
- Eine gegebenenfalls sinnvolle Herausgabe von vertraulichen Informationen an einen Dritten, z.B. an einen Dienstleister oder Projektpartner, erfolgt immer über eine*n autorisierten Mitarbeiter*in des ESH.

4.1.4 PASSWÖRTER UND BERECHTIGUNGEN

- Die Zugriffsmöglichkeiten auf Daten sind bewusst abteilungs-, gruppen- oder projektbezogen eingeschränkt.
- Die Zugriffsmöglichkeiten auf sicherheitsrelevante Daten sowie der Zutritt zu sicherheitsrelevanten Bereichen darf nur Berechtigten ermöglicht werden. Der Kreis der jeweils Berechtigten wird vom beauftragenden Bereich des ESH festgelegt.
- Eine gegebenenfalls mögliche Umgehung der Zugriffsbeschränkung stellt eine klare Verletzung dieser Richtlinie dar.
- Insbesondere Passwörter oder sonstige Zugangskennungen dürfen niemals anderen zugänglich gemacht werden, auch nicht anderen Mitarbeiter*innen oder Administrator*innen. Lediglich Administrator*innen, die für die Verwaltung von Passwörtern und Zugangsberechtigungen verantwortlich sind, dürfen diese ausstellen und an die jeweiligen Benutzer*innen ausgeben.
- Die von der/dem Benutzer*in gewählten Passwörter sollen komplex sein, d.h. sie sollen nicht einfach zu erraten sein (siehe hierzu 5.1)
- Das Vorhalten der Passwörter in schriftlicher oder elektronischer Form ist unzulässig. Ausgenommen ist dem aktuellen Stand der Sicherheitstechnik entsprechende Software zur Verwaltung von Passwörtern.
- Das Passwort ist umgehend zu wechseln, wenn der Verdacht besteht, dass es anderen Personen bekannt geworden ist.
- Die unberechtigte Weitergabe von Authentisierungen (z.B. Benutzername und Passwort, Zugangskarte, OTP-Token, etc.) stellt eine Verletzung dieser Richtlinie dar.
- Ein entsprechender Prozess regelt die Vergabe und Rücknahme der notwendigen Berechtigungen, die für die Erfüllung der fachlichen Aufgaben erforderlich sind.
- Benutzerberechtigungen werden automatisiert nach einem definierten Zeitraum gesperrt. Der Zeitraum richtet sich nach der Projektlaufzeit bzw. den für die Unterstützung erforderlichen Zeitrahmen. Ist der definierte Zeitraum überschritten worden, kann der/die Dienstleister*in sich an den/die jeweilige*n Ansprechpartner*in wenden.

4.1.5 HARD- UND SOFTWARE

- Es darf grundsätzlich nur sachbezogene, korrekt lizenzierte Hard- und Software benutzt werden.
 - Administrator*innen sowie Dienstleistungsmitarbeiter*innen haben eine besondere Sorgfaltspflicht und eine entsprechende Vorsorge zu treffen, wenn diese Patches, Updates oder sonstige neue Software herunterladen, installieren oder testen. Das Changemanagement des ESH ist mit einzubeziehen.

4.1.6 EINSATZ VON FREMDHARDWARE UND FREMDSOFTWARE

Nicht durch das ESH beschaffte Hard- und Software, die ein*e Dienstleistungsmitarbeiter*in im Rahmen ihrer/seiner Tätigkeit vor Ort einsetzen möchte wird als Fremdhardware und Fremdsoftware bezeichnet. Der Einsatz ist nur unter folgenden Bedingungen zulässig:

- Der Einsatz der Fremdhardware und Fremdsoftware vor Ort muss durch das ESH vor dem Einsatz freigegeben worden sein.
- Das verwendete Betriebssystem muss auf einem aktuellen Sicherheitsstand sein – es müssen alle notwendigen Sicherheitspatches eingespielt sein.
- Auf dem System muss ein Virens Scanner installiert und aktiv sein, der dem allgemeinen Stand der Technik entspricht. Dessen Viren-Signaturen dürfen nicht älter als 1 Tag sein und sich regelmäßig, möglichst täglich, aktualisieren.
- Datenträger, die in Systemen des ESH eingesetzt werden sollen, wie z.B. CD/DVDs, USB-Sticks, externe Festplatten etc., sind vorher auf Viren-Freiheit zu überprüfen.
- Die eingesetzte Fremdhardware darf bei einem Betrieb im Netzwerk des ESH keine parallelen Netzwerkkopplungen, z.B. über Modem, ISDN, Funknetze etc., zu fremden Netzen aufbauen oder halten.
- Die/der Dienstleistungsmitarbeiter*in verpflichtet sich, keine Programme oder Programmteile zur Ausführung zu bringen, die wesentlich den Produktionsbetrieb signifikant einschränken oder einen Schaden verursachen können.

4.1.7 E-MAIL, INTERNET UND TELEKOMMUNIKATION

- Alle geschäftsrelevanten elektronischen Daten und Informationen müssen auf den zentralen Server-Systemen des ESH gespeichert werden. Eine Speicherung in einem persönlichen Bereich (lokale Festplatte oder Home-Laufwerk, externe Speichermedien etc.) ist nicht gestattet.
- Die private Nutzung von Email, Internet-Diensten (Web-Seiten, Messenger, Streaming, etc.) sowie von Telefon oder sonstigen Telekommunikationsdiensten ist grundsätzlich nicht gestattet.

4.1.8 SICHERHEITSVORFÄLLE

Erkannte Sicherheitslücken, Sicherheitsverletzungen und Sicherheitsvorfälle, dazu gehören z.B.

- Befall durch Viren, Trojaner und Würmer,
- ungenutzte, aktive Accounts ausgeschiedener Mitarbeiter*innen,
- Angriffe auf die IT-Systeme,
- Verlust von IT-Systemen oder Mobile Devices,

müssen unverzüglich an den Kundenservice oder der Stabsstelle ISMS gemeldet werden. Dies kann mündlich oder formlos per Email über die nachstehenden Kontaktdaten erfolgen:

Service Desk

Tel.: 0201 88-17188

Email: servicedesk@esh.essen.de

Stabsstelle ISMS

Email: informationssicherheit@esh.essen.de

In Zweifelsfällen, bei denen nicht klar ersichtlich ist, ob es sich um einen Sicherheitsvorfall handelt oder nicht, ist zunächst ein Sicherheitsvorfall anzunehmen und unverzüglich zu melden.

Erkannte Sicherheitslücken und Sicherheitsverletzungen sind auch dann an die Stabsstelle ISMS oder an den Kundenservice zu melden, wenn die/der Dienstleistungsmitarbeiter*in, z.B. aufgrund vorangegangener Erfahrungen, nicht mit einer Änderung der Situation rechnet.

5 AUTHENTISIERUNG

5.1 KENNWORTALTER UND KENNWORTKOMPLEXITÄT

Um ein einfaches Ausforschen von Kennwörtern zu erschweren und einer Verbreitung von Kennwörtern über einen längeren Nutzungszeitraum zu erschweren, sind folgende Regeln zur Kennwortnutzung in den Systemen des ESH einzuhalten:

- Länge von mindestens zwölf (12) Zeichen.
- Kennwortkomplexität:
Das Kennwort muss Zeichen aller vier folgenden Kategorien enthalten:
 - Ziffer
 - Großbuchstaben
 - Kleinbuchstaben
 - Sonderzeichen.
- Kennwörter dürfen keine persönlichen Daten enthalten (z.B. Geburtsdatum, Adresse, Name von Familienmitgliedern, etc.).
- Kennwörter dürfen keine Trivialkennwörter und gängige Zeichenketten darstellen (z. B. "123456", "password", "asdf", etc.).
- Ab einer Länge von 25 Zeichen gilt ein Kennwort als Passphrase. Diese muss aus Groß- und Kleinbuchstaben bestehen und kann Leerzeichen enthalten.

Bei Systemen mit besonderen Sicherheitsanforderungen gelten ggf. abweichende Regelungen.

6 KLASSIFIZIERUNG VON DATEN UND INFORMATIONEN

Alle Daten und Informationen sind gemäß ihrer jeweiligen Klassifizierung zu behandeln und dürfen nur berechtigten Personen zugänglich gemacht werden. Dazu wird allen Daten und Informationen eine der folgenden Klassifizierungsstufen zugewiesen:

- **ÖFFENTLICH:** Dokumente, Daten und Informationen dieser Vertraulichkeitsstufe dürfen der Öffentlichkeit zugänglich gemacht werden, z. B. im Internet oder in Prospekten und Broschüren für die Öffentlichkeitsarbeit; eine Vertraulichkeit dieser Informationen ist nicht gefordert.
- **INTERN:** Dokumente, Daten und Informationen, die nur für den internen Gebrauch, sowie innerhalb des Konzerns und nicht für die allgemeine Öffentlichkeit bestimmt sind. Dienstliche Kommunikationsdaten (z.B. Vorgaben zum Arbeitsschutz, selbst entwickelte Schulungsunterlagen, Anleitungen, Dienstanweisungen) Konsequenzen beim Verlust der Vertraulichkeit sind denkbar, jedoch geringfügiger Natur.
- **VERTRAULICH:** Diese Klassifizierung wird für Dokumente, Daten und Informationen vergeben, die nur für den internen Gebrauch durch einen eingeschränkten, klar umrissenen Personenkreis bestimmt sind, wie z. B. Betriebshandbücher.
- **STRENG VERTRAULICH:** Informationen, die als streng vertraulich klassifiziert sind, dürfen nur einem begrenzten, klar definierten Personenkreis zugänglich sein. Sie dürfen durch Dienstleister*innen an niemanden weitergegeben werden, wie z. B. Passwörter, Pentestberichte.

Alle nicht klassifizierten bzw. nicht entsprechend gekennzeichneten Dokumente sind automatisch als INTERN eingestuft. Alle übrigen Dokumente müssen ausdrücklich gekennzeichnet werden, also auch Dokumente mit der Einstufung als ÖFFENTLICH. Die Vertraulichkeit muss zudem auch über den Nutzungszeitraum hinaus (z.B. bei der Entsorgung) sichergestellt werden. Bei Unklarheiten im Umgang mit Dokumenten, Daten und Informationen im Rahmen der Auftragsausführung steht die*der jeweilige Ansprechpartner*in zu Verfügung.

7 VERHALTEN BEI UNREGELMÄßIGKEITEN

Alle Erkenntnisse über sicherheitsrelevante Vorkommnisse und Sicherheitsverstöße sind grundsätzlich als streng vertraulich zu behandeln und unverzüglich dem Informationssicherheitsbeauftragten oder seiner Stellvertretung zu melden. Die Weitergabe dieser Erkenntnisse an Dritte, z.B. Betriebsfremde, ist untersagt und stellt einen groben Verstoß gegen diese Richtlinie dar. In jedem Fall ist bei Verstößen sofort zu reagieren und es sind angemessene Maßnahmen gegen die/den Verursacher*in zu ergreifen.

8 DATENSCHUTZ

Personenbezogene Daten unterliegen einem besonderen gesetzlichen Schutz. Um diese Daten zu schützen, gilt es die Regeln zur Verarbeitung (das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung) sowie Nutzung gemäß den gesetzlichen Vorgaben zu beachten. Alle Dienstleistungsmitarbeiter*innen sind im Rahmen ihrer Tätigkeit für das ESH deshalb dazu verpflichtet, die personenbezogenen Daten anderer vertraulich und weisungsgerecht zu behandeln. Die Dienstleistungsmitarbeiter*innen sind dafür verantwortlich, dass die Ihnen anvertrauten personenbezogenen Daten nur im Rahmen Ihrer Aufgabenstellung erhoben, verarbeitet oder genutzt werden. Jeder Missbrauch und jede unbefugte Weitergabe dieser Daten sind unzulässig und zudem strafbar. Zur Wahrung des Schutzes von personenbezogenen Daten sind insbesondere folgende Regelungen zu beachten:

- Es ist untersagt, geschützte personenbezogene Daten unbefugt zu einem anderen als zu dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu erheben, zu verarbeiten, bekannt zu geben, zugänglich zu machen oder sonst zu nutzen. Diese Untersagung besteht auch nach Beendigung der Tätigkeit für das ESH fort.
- Beim Umgang mit personenbezogenen Daten, insbesondere bei der Verarbeitung und Sicherung personenbezogener Daten, sind bestehende Anweisungen zu beachten.
- Zum Schutz personenbezogener Daten ist im Rahmen der zugewiesenen Aufgabe die erforderliche Sorgfalt anzuwenden; festgestellte Mängel sind der/dem jeweiligen Ansprechpartner*in oder der Stabsstelle ISMS unverzüglich zu melden.

Dienstleistungsmitarbeiter*innen haben die anvertrauten Daten und Datenträger unter Verschluss zu halten, wenn sie nicht unmittelbar daran arbeiten. Zudem dürfen die IT-Systeme, die IT-Anwendungen und die Passwörter keinem Unbefugten zugänglich gemacht werden. Nicht mehr benötigte Datenträger mit personenbezogenen Daten müssen datenschutzgerecht vernichtet werden, um eine missbräuchliche Nutzung zu verhindern.

Bei Beendigung des Dienstleistungsverhältnisses ist die/der Dienstleistungsmitarbeiter*in verpflichtet:

- jegliche, dem ESH gehörenden Software-Komponenten, Daten, Dokumentationen, Auswertungen usw. von nicht ESH eigenen IT-Systemen zu löschen,
- dem ESH gehörende Software-Komponenten weder privat noch geschäftlich weiter zu nutzen,
- keine elektronischen, papiergebundene oder sonstige Kopien von Software Komponenten und Daten des ESH mehr zu besitzen,
- alle eventuell vorhandenen elektronischen, papiergebundene oder sonstige Kopien an das ESH zurückzugeben.

Für Schäden, die aufgrund der Missachtung dieser Richtlinien entstehen, kann der Verursacher in vollem Umfang haftbar gemacht werden.

10 SANKTIONEN

Verstöße gegen diese Richtlinie werden mit einer Beendigung der Dienstleistung geahndet. Das ESH behält sich im Falle eines Verstoßes die vollständige Rückabwicklung des Dienstleistungsvertrages vor. Bei gesetzlichen Verstößen erfolgt in jedem Fall eine Meldung an die jeweils zuständige Ermittlungsbehörde. Straftaten werden zur Anzeige gebracht und werden strafrechtlich verfolgt.

Verpflichtungserklärungen

Ich _____,

Mitarbeiter/-in der Firma _____ habe die „Dienstleisterrichtlinie zur Nutzung der IT-Infrastruktur des ESH“ in der Version 2.2 vom 14.10.2025 erhalten und verpflichte mich durch meine Unterschrift zur Einhaltung dieser Dienstleisterrichtlinie.

Weiterhin verpflichte ich mich, alle im Rahmen meiner Tätigkeit beim ESH erlangten Informationen vertraulich zu behandeln. Die Einhaltung dieser „Dienstleisterrichtlinie zur Nutzung der IT-Infrastruktur des ESH“ ist ein wesentlicher Bestandteil meiner Dienstleistung für das ESH.

Durch diese Verpflichtungen werden bereits bestehende sonstige Geheimhaltungspflichten nicht beeinträchtigt.

Ort: _____, den _____

Unterschrift: _____