

ISMS Sicherheitsrichtlinie für Fremddienstleister

Zusammenfassung	ISMS Sicherheitsrichtlinie legt Regelungen für Fremddienstleister im Netzbetrieb fest.
------------------------	----------------------------------------------------------------------------------------

Managementsystem	ISO/IEC 27001
Version	1.1
Version vom	01.08.2024
Status	freigegeben
Klassifizierung	Öffentlich
Zentralisierung	keine

Dok. Owner Orga	ISMS-B
Prüfung durch Orga	ISMS-B
Freigabe durch Orga	ISMS-B

Änderungshistorie

Vers.	Änderungen	Name Orga	Rolle*	Datum
1.1	Erstellung	R. Aichele	B/F	01.08.2024

*) Rollen: (B)earbeitung, (P)rüfung, (F)reigabe.
 Fachprüfungen und Freigaben finden nach erstmaliger Freigabe nur bei wesentlichen Änderungen des Bearbeiters statt.

Inhalt

1. Geltungsbereich
2. Eingesetztes Personal
3. Zutrittsrechte
4. Zugangs- und Zugriffsrechte
5. Einsatz von Hard- und Software des Dienstleisters
6. Kopplung von Systemen des Dienstleisters
7. Sicherer Datenaustausch
8. Sicherheit von Daten beim Dienstleister
9. Zur Verfügung gestellte Hilfsmittel
10. Verwendung von Datenträgern
11. Informationssicherheitsvorfälle und Schwachstellen
12. Remote Access Anbindungen
13. Lieferung von Software
14. Lieferung von Hardware
15. Einhaltung der Richtlinie u.a. bei Subunternehmen
16. Überprüfung der Einhaltung der Vorgaben

1. Geltungsbereich

Die ISMS Sicherheitsrichtlinie legt die Regelungen für Dienstleister im Bereich des Netzbetriebs der ENO fest. Die Sicherheitsrichtlinie gilt für alle Mitarbeiter des Auftragnehmers, die mit der Aufgabenerfüllung eingebunden sind.

2. Eingesetztes Personal

Der Auftragnehmer stellt sicher, dass für die Arbeiten nur qualifiziertes Personal zum Einsatz kommt.

3. Zutrittsrechte

Zutrittsrechte werden Personen nur in besonderen Fällen erteilt. Im Normalfall erfolgt ein Zutritt für Dienstleister immer begleitet durch Mitarbeiter des Auftraggebers. Mitarbeiter des Dienstleisters haben sich an die Weisungen des Auftraggebers zu halten. Vor dem Zutritt zu technischen Anlagen erfolgt eine Unterweisung des Dienstleisters durch den Auftraggeber.

4. Zugangs- und Zugriffsrechte

Zugangs- und Zugriffsrechte sind auf das minimal notwendige Maß zu beschränken und durch personalisierte Accounts auszuführen. Alle Zugangs- und Zugriffsrechte der Dienstleister sind mit dem Auftraggeber abzustimmen und vorab zu genehmigen.

Zugewiesene Rechte dürfen ausschließlich für die jeweilige Aufgabenerfüllung benutzt werden. Jeder Mitarbeiter hat ausschließlich seinen personalisierten Account zu benutzen. Passwörter sind sicher zu verwahren. Eine Weitergabe von Passwörtern ist verboten.

Dienstleister haben die zuständige Fachabteilung umgehend zu informieren, wenn ein Zugang/Zugriff nicht mehr benötigt wird (z.B. Auftragsabschluss oder Mitarbeiter hat das Unternehmen verlassen). Benötigt ein Dienstleister Administrationsrechte muss dieses durch den zuständigen Fachbereich genehmigt und eingerichtet werden. Hierzu ist die Unterzeichnung einer Administratorenverpflichtungserklärung notwendig. Alle administrativen Arbeiten sind detailliert mit dem Auftraggeber abzustimmen.

5. Einsatz von Hard- und Software des Dienstleisters

Setzt der Dienstleister eigene Hard- oder Software für den Auftraggeber ein, ist dies vorab durch den Auftraggeber zu genehmigen. Das Verwenden von Software durch den Dienstleister beim Auftraggeber muss durch den Dienstleister lizenzrechtlich sichergestellt sein. Die eingesetzte Software ist auf den aktuellen Stand zu halten.

6. Kopplung von Systemen des Dienstleisters

Das Koppeln von Systemen des Dienstleisters mit den Anlagen des Auftraggebers ist nur in Ausnahmefällen zulässig. Der Dienstleister darf ohne die Genehmigung des Auftraggebers keine Systeme koppeln. Vor der Kopplung sicher zu stellen, dass die Systeme des Dienstleisters auf Schadsoftware geprüft sind.

7. Sicherer Datenaustausch

Datenaustausch zwischen dem Dienstleister und dem Auftraggeber hat sicher zu erfolgen. Welche Verfahren einzusetzen sind, ist abhängig von der Einstufung der Daten, die übertragen werden sollen. Das Verfahren ist im Vorfeld zwischen Auftraggeber und Dienstleister abzustimmen. Grundsätzlich sollte eine verschlüsselte Datenübertragung stattfinden. Ein Datenaustausch über Sharepoint kann durch den Auftraggeber eingerichtet werden.

8. Sicherheit von Daten beim Dienstleister

Daten beim Dienstleister müssen gegen den Zugriff durch Unberechtigte geschützt sein. Der Zugriff auf die Daten muss auf das betriebsnotwendige Maß eingeschränkt sein. Der Dienstleister ist verpflichtet, geeignete Maßnahmen gegen Datenverlust zu ergreifen.

Die Daten des Auftraggebers dürfen beim Dienstleister ausschließlich auf Systemen innerhalb der EU verarbeitet oder gespeichert werden.

Daten dürfen durch den Dienstleister nicht an Dritte weitergegeben werden. Sollte dies dennoch notwendig werden, ist dies durch den Auftraggeber zu genehmigen.

Daten sind über einen aktuellen Virenschanner zu prüfen.

9. Zur Verfügung gestellte Hilfsmittel

Stellt der Auftraggeber dem Dienstleister Hilfsmittel wie z.B. Hard- oder Software, Pläne, sonstige Unterlagen zur Aufgabenerfüllung zur Verfügung, sind diese, wenn sie durch den Dienstleister nicht mehr benötigt werden bzw. spätestens nach Ende der Arbeiten/Auftrags zurückzugeben bzw. zu vernichten.

Die Übergabe/Rückgabe von Hilfsmitteln ist durch den Auftraggeber zu dokumentieren und durch den Dienstleister schriftlich zu bestätigen.

10. Verwendung von Datenträgern

Datenträger sind grundsätzlich zu verschlüsseln und vor Verwendung auf Schadsoftware zu prüfen.

11. Informationssicherheitsvorfälle und Schwachstellen

Bekommt ein Dienstleister Kenntnis eines Informationssicherheitsvorfall oder einer –Schwachstelle bei dem Auftraggeber, ist dieser unverzüglich darüber zu informiere. Passiert beim Dienstleister ein Informationssicherheitsvorfall, der in Zusammenhang mit den Arbeiten oder Daten des Auftraggebers steht oder Auswirkung darauf haben könnte, ist der Auftraggeber ebenfalls unverzüglich darüber zu informieren.

12. Remote Access Anbindungen

Remote Access Anbindungen sind durch den Auftraggeber zu genehmigen. Mitarbeiter des Dienstleisters, die sich über Remote Zugriffe auf Anlagen des Auftraggebers aufschalten können, sind im Vorfeld zu benennen. Es erfolgt eine Protokollierung und ggf. eine Auswertung der Tätigkeiten durch den Auftraggeber.

Der Dienstleister stellt sicher, dass die vorhanden Remote Access Anbindungen in seinem Verantwortungsbereich nicht missbräuchlich verwendet werden.

13. Lieferung von Software

Bei der Lieferung von Software, Programmen, Quellcode und Parametrierfiles hat der Dienstleister sicherzustellen, dass die ausgelieferte Software frei von Schadsoftware ist.

Die Software ist vor Auslieferung durch den Dienstleister zu prüfen, dass der festgelegte Funktionsumfang (inkl. Sicherheitsfunktionen) gegeben ist. Ist die Software durch den Dienstleister entwickelt worden, muss der Dienstleister sicherstellen, dass keine Backdoors eingebaut wurden. Bei der Installation der Software ist darauf zu achten, dass nur die benötigte Software installiert wird. Jegliche Teile der Software oder Hilfsprogramme der Entwicklung dürfen nicht installiert werden. Nur beauftragte und benötigte Softwarefunktionen sind zu aktivieren bzw. zu installieren. Die Software ist zu versionieren und bei Updates die Änderungen über Release Notes dem Auftraggeber mitzuteilen.

Sind in der Software Schwachstellen bekannt, sind diese durch Dienstleister zu beseitigen bzw. der Auftraggeber ist darüber zu informieren. Sollte Software im Einsatz sein, für die durch den Hersteller keine Sicherheitsupdates mehr zur Verfügung gestellt werden, ist dies dem Auftraggeber mitzuteilen.

Der Auftraggeber ist darüber zu informieren, wenn Systempasswörter, Herstellerpasswörter oder Passwörter des Dienstleisters mit ausgeliefert werden.

14. Lieferung von Hardware

Bei der Lieferung von Hardware hat der Dienstleister sicher zu stellen, dass es sich bei der Hardware um Originale handelt. Sind bei dem ausgelieferten Produkt Sicherheitsschwachstellen bekannt, sind diese durch den Dienstleister zu beseitigen bzw. der Auftraggeber ist darüber zu informieren.

Der Auftraggeber ist darüber zu informieren, wenn Systempasswörter, Herstellerpasswörter oder Passwörter des Dienstleisters mit ausgeliefert werden.

15. Einhaltung der Richtlinie u.a. bei Subunternehmen

Der Einsatz von Subunternehmen ist vom Auftragnehmer anzuzeigen. Der Auftragnehmer sorgt innerhalb seines Unternehmens und bei seinen Subunternehmen für die Beachtung dieser Sicherheitsrichtlinie. Die ISMS Sicherheitsrichtlinie für Fremddienstleister ist allen eingesetzten Subunternehmen durch den Auftragnehmer bekannt zu geben und mit Unterschrift bestätigen zu lassen.

16. Überprüfung der Einhaltung der Vorgaben

Die Einhaltung der Vorgaben dieser Richtlinie können jederzeit durch Mitarbeiter der ENO GmbH bei den Mitarbeitern des Dienstleisters überprüft werden. Dies kann auch durch eine Prüfung der Einhaltung an den Standorten des Dienstleisters beinhalten.

Kenntnisnahme des Dienstleisters:

Dienstleister / Firma

Datum

Unterschrift