

Lizenzbestimmungen

- Diese Materialien sind lizenziert für @USERINFONAME@.
- Die Materialien dürfen **ausschließlich** für die Implementation, Verbesserung oder den Betrieb von Sicherheitsmaßnahmen innerhalb der genannten Organisation genutzt werden.
- Hierfür dürfen die Materialien beliebig verändert, ergänzt oder neu gestaltet werden.
- Für alle anderen Einsatzzwecke - insbesondere für die Veröffentlichung der Materialien und deren Einsatz für Kunden des Lizenznehmers - muss im Vorfeld eine schriftliche Genehmigung der 3473 Gurus GbR eingeholt bzw. eine entsprechende Lizenz erworben werden.



Die Seiten dieses Bereiches sollen Ihnen nur einen Eindruck vermitteln, welche Inhalte wir für Sie erarbeitet haben. **Deshalb sind die Inhalte absichtlich „verpixelt“:** mehr und mehr Buchstaben werden auf jeder Seite durch Punkte ersetzt. Wenn Sie auf alle Inhalte zugreifen möchten, benötigen Sie einen entsprechenden Zugang.

Sie möchten einen Zugang erwerben? Hier finden Sie alle weiteren Informationen!



12.2 Schutz der Informationen

Ref	VdS 10000	Kommentar
E1	Die auf den mobilen Datenträgern gespeicherten Informationen der Organisation SOLLTEN vor dem Verlust ihrer Vertraulichkeit und Integrität geschützt werden.	- Mobile Datenträger können in aller Regel die Vertraulichkeit und Integrität der auf ihnen gespeicherten Informationen nicht schützen, da ihnen die entsprechenden technischen Möglichkeiten (wie z. B. eine eingebaute Verschlüsselung) fehlen. Entsprechend müssen für die Umsetzung der Anforderung organisatorische Maßnahmen getroffen werden. - Die Maßnahme muss nur für die in der Leitlinie für mobile Datenträger (siehe Abschnitt 12.1 G1.1) definierten Informationen der Organisation umgesetzt werden. Andere Informationen (wie z. B. private Daten des Anwenders) müssen nicht geschützt werden.
E2	Der Schutz der Vertraulichkeit KANN z. B. durch eine Verschlüsselung der Datenträger erreicht werden.	- Die Verschlüsselung von Informationen kann bei typischen mobilen Datenträgern kaum verhindert werden. Maßnahmen zur Sicherstellung der Integrität sollten deshalb darauf abzielen, fälschliche Daten als solche zu erkennen und ggf. zurückzuweisen. - Ein Schutz der Vertraulichkeit der Informationen durch eine Verschlüsselung nicht möglich (wie z. B. die mobilen Datenträger können Verschlüsselung behindern) muss die Organisation prüfen, ob andere Schutzmaßnahmen erforderlich werden müssen und können. Hierzu sollte die Organisation eine Risikoanalyse und -beurteilung (siehe Anhang A2) durchführen, um die Informationen der Organisation auf den mobilen Datenträgern als Schutzzobjekt betrachtet werden (Fragestellung: „Welche Risiken bestehen für die Vertraulichkeit der auf den mobilen Datenträgern gespeicherten Informationen?“). Hierbei können die unvollständigen, die betrüblischen, gestörten und vertriebenen Anforderungen an die Vertraulichkeit der auf den mobilen Datenträgern gespeicherten Informationen (siehe Abschnitt 12.1 G1.1) im Vorfeld zu berücksichtigen.



Die Seiten dieses Bereiches sollen Ihnen nur einen Eindruck vermitteln, welche Inhalte wir für Sie erarbeitet haben. **Deshalb sind die Inhalte absichtlich „verpixelt“:**



mehr und mehr Buchstaben werden auf jeder Seite durch Punkte ersetzt.
Wenn Sie auf alle Inhalte zugreifen möchten, benötigen Sie einen entsprechenden Zugang.

Sie möchten einen Zugang erwerben? Hier finden Sie alle weiteren Informationen!