IKT-Sicherheitsrichtlinie

[Thema EINFÜGEN]

Versionsnummer: *[Versionsnummer EINFÜGEN]*

Freigabedatum durch das Leitungsorgan: *[DD.MM.JJJJ]*

Kommentiert [MH1]: ***DORA-Anforderung:*** *Stellen Sie sicher, dass die IKT-Sicherheitsrichtlinien das Datum der formellen Genehmigung durch das Leitungsorgan angeben*

DORA-Referenz Art. 2 (2b) RTS risk mgt.: *Financial entities shall ensure that the ICT security policies referred to in paragraph 1: indicate the date of the formal approval of th ICT security policies by the management body;*

DORA-Anforderung: *Das Leitungsorgan soll Richtlinien implementieren, um hohe Standards bei der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten sicherzustellen.*

DORA-Referenz Art. 5 (2b) DORA: *The management body of the financial entity shall define, approve, oversee and be responsible for the implementation of all arrangements related to the ICT risk management framework referred to in Article 6(1). For the purposes of the first subparagraph, the management body shall put in place policies that aim to ensure the maintenance of high standards of availability, authenticity, integrity and confidentiality, of data;*

Inhalt

Änderungshistorie

Datum	Version	Beschreibung der Änderimg	Grund für die Änderung	Autor
DD.MM.JJJJ	V1.0	Initiale Erstellung		M. Hofmann

Einleitung

Zweck der Richtlinie

[Erläuterung, warum die Richtlinie erstellt wurde und welche Ziele damit verfolgt werden.]

Geltungsbereich

[Beschreibung der Abteilungen, Mitarbeiter oder Prozesse, auf die die Richtlinie Anwendung findet.]

Bezug zur DOR-Strategie

[Beschreibung der Informationssicherheitsziele und der relevanten Bezüge zur DOR-Strategie.]

Grundsätze der Proportionalität

[Beschreibung der Berücksichtigung von Größe, Risiko-Profil und Komplexität bei der IKT-Sicherheitsrichtlinie.]

Kommentiert [MH2]: ***DORA-Anforderung:*** *Stellen Sie sicher, dass die IKT-Sicherheitsrichtlinien mit den Informationssicherheitszielen der DOR-Strategie übereinstimmen.*

DORA-Referenz Art. 2 (2a) RTS risk mgt.
Financial entities shall ensure that the ICT security policies referred to in paragraph 1: are aligned to the financial entity's information security objectives included in the digi operational resilience strategy referred to in Article 6(8) of Regulation (EU) 2022/2554;

Kommentiert [MH3]: ***DORA-Anforderung:***
Implementieren Sie die DORA-Anforderungen proportional unter Berücksichtigung der Größe, des Risikoprofils sowie d Art, des Umfangs und der Komplexität der Dienstleistunge Aktivitäten und Operationen.

DORA-Referenz Art. 4 (1 & 2) DORA:
Art. 4(1): Financial entities shall implement the rules laid down in Chapter II in accordance with the principle of proportionality, taking into account their size and overall r profile, and the nature, scale and complexity of their servic activities and operations.
Art. 4(2): In addition, the application by financial entities o Chapters III, IV and V, Section I, shall be proportionate to th size and overall risk profile, and to the nature, scale and complexity of their services, activities and operations, as specifically provided for in the relevant rules of those Chapters.

DORA-Referenz Art. 1 RTS risk mgt.: *When developing and implementing the ICT security policies, procedures, protoco and tools referred to in Title II and the simplified ICT risk management framework referred to in Title III, the size and the overall risk profile of the financial entity, and the natur scale and elements of increased or reduced complexity of i services, activities and operations shall be taken into account[…]*

Dokumentenlenkung

Änderung & Überprüfung

[Beschreibung der Änderungs- und Überprüfungsvorgaben]

Genehmigung und Freigabe

[Beschreibung der Genehmigungs- und Freigabeprozesse durch das Leitungsorgan]

Veröffentlichung

[Beschreibung der Veröffentlichungsprozesse und des Veröffentlichungsortes]

Kommentiert [MH4]: ***DORA-Anforderung:*** *Stellen Sie sicher, dass die IKT-Sicherheitsrichtlinien mindestens jährlich sowie nach größeren IKT-Vorfällen, behördlichen Anweisungen oder Resilienztests und Audits überprüft werden.*

DORA-Referenz Art. 2 (2j) RTS risk mgt.:
Financial entities shall ensure that the ICT security policies referred to in paragraph 1 are reviewed in accordance with Article 6(5) of Regulation (EU) 2022/2554;

DORA-Referenz Art. 6 (5) DORA: *The ICT risk management framework shall be documented and reviewed at least once a year, or periodically in the case of microenterprises, as well as upon the occurrence of major ICT-related incidents, and following supervisory instructions or conclusions derived from relevant digital operational resilience testing or audit processes. It shall be continuously improved on the basis of lessons derived from implementation and monitoring. A report on the review of the ICT risk management framework shall be submitted to the competent authority upon its request.*

DORA-Anforderung: *Stellen Sie sicher, dass die IKT-Sicherheitsrichtlinien wesentliche Änderungen in der Finanzinstitution berücksichtigen, einschließlich Änderungen bei Aktivitäten und Prozessen, Cyber-Bedrohungen oder rechtlichen Verpflichtungen.*

DORA-Referenz Art. 2 (2k) RTS risk mgt.:
Financial entities shall ensure that the ICT security policies referred to in paragraph 1 take into account material changes concerning the financial entity, including material changes to the activities or processes of the financial entity, to the cyber threat landscape, or to applicable legal obligations.

Kommentiert [MH5]: ***DORA-Anforderung:*** *Das Leitungsorgan soll das IKT-Risikomanagement-Rahmenwerk definieren, genehmigen, überwachen und dessen Implementierung sicherstellen.*

DORA-Referenz Art. 5 (2) DORA: *The management body of the financial entity shall define, approve, oversee and be responsible for the implementation of all arrangements related to the ICT risk management framework referred to in Article 6(1).*

Einhaltung und Kontrolle der Vorgaben

Risiken und Kontrollen

[Beschreibung der Risiken und Kontrollen, die die Einhaltung der Richtlinie sicherstellen.]

Implementierungsindikatoren

[Beschreibung der Implementierungsindikatoren und Überwachungsmaßnahmen.]

Maßnahmen bei Nichteinhaltung

[Beschreibung der Konsequenzen und Folgen der Nichteinhaltung der Richtlinie.]

Kommentiert [MH6]: ***DORA-Anforderung:*** *Richten Sie e internes Governance- und Kontrollrahmenwerk ein, um ein effektives IKT-Risikomanagement sicherzustellen und eine hohe digitale operative Resilienz zu erreichen.*

DORA-Referenz Art. 5 (1) DORA*: Financial entities shall ha in place an internal governance and control framework tha ensures an effective and prudent management of ICT risk, accordance with Article 6(4), in order to achieve a high lev of digital operational resilience.*

Kommentiert [MH7]: ***DORA-Anforderung:*** *Stellen Sie sicher, dass die IKT-Sicherheitsrichtlinien Indikatoren und Maßnahmen enthalten, um (i) die Implementierung von IK Sicherheitsrichtlinien, -verfahren, Protokollen und Tools zu überwachen; (ii) Ausnahmen von IKT-Sicherheitsrichtlinien dokumentieren und (iii) die digitale operative Resilienz im Falle solcher Ausnahmen zu gewährleisten.*

DORA-Referenz Art. 2 (2c) RTS risk mgt.:
Financial entities shall ensure that the ICT security policies referred to in paragraph 1 contain indicators and measure to (i) monitor the implementation of the ICT security polici procedures, protocols, and tools; (ii) record exceptions fron that implementation and (iii)
ensure that the digital operational resilience of the financi entity is ensured in case of exceptions as referred to in poi (ii);

Kommentiert [MH8]: ***DORA-Anforderung:*** *Stellen Sie sicher, dass die IKT-Sicherheitsrichtlinien die Folgen von Nichteinhaltung durch das Personal festlegen, falls diese nicht durch andere Richtlinien der Finanzinstitution abgedeckt sind.*

DORA-Referenz Art. 2 (2e) RTS risk mgt.: *Financial entities shall ensure that the ICT security policies referred to in paragraph 1 specify the consequences of non-compliance staff of the financial entity with the ICT security policies, where provisions to that effect are not laid down in other policies of the financial entity;*

IKT-Sicherheitsvorgaben

Definitionen

[Beschreibung der für die IKT-Richtlinie relevanten Definitionen]

Rollen und Verantwortlichkeiten

[Beschreibung von klaren Rollen und Verantwortlichkeiten für alle ICT-bezogenen Funktionen]

Segregation of Duties

[Beschreibung der relevanten Aspekte zur Funktionstrennung]

Standards und Best Pracitices

[Beschreibung der relevanten Standards und Best Practices]

Inhaltliche Vorgaben

[Beschreibung der inhaltlichen Vorgaben der IKT-Richtlinie]

Schulung und Kommunikation

[Beschreibung der Schulungsmaßnahmen und Kommunikationsstrategien, um sicherzustellen, dass alle Mitarbeiter über die Richtlinie informiert sind und wissen, wie sie diese umsetzen können]

Kommentiert [MH9]: ***DORA-Anforderung:*** *Stellen Sie sicher, dass die IKT-Sicherheitsrichtlinien die Verantwortlichkeiten des Personals auf allen Ebenen für di Gewährleistung der IKT-Sicherheit festlegen.*

DORA-Referenz Art. 2 (2d) RTS risk mgt.:
Financial entities shall ensure that the ICT security policies referred to in paragraph 1:
specify the responsibilities of staff at all levels to ensure th financial entity's ICT security;

DORA-Anforderung: *Das Leitungsorgan soll klare Rollen u Verantwortlichkeiten für alle IKT-bezogenen Funktionen festlegen und eine angemessene Governance einrichten, u eine effektive und rechtzeitige Kommunikation, Zusammenarbeit und Koordination dieser Funktionen zu gewährleisten.*

DORA-Referenz Art. 5 (2c) DORA:
The management body of the financial entity shall define, approve, oversee and be responsible for the implementatio of all arrangements related to the ICT risk management framework referred to in Article 6(1). For the purposes of t first subparagraph, the management body shall set clear roles and responsibilities for all ICT-related functions and establish appropriate governance arrangements to ensure effective and timely communication, cooperation and coordination among those functions;

Kommentiert [MH10]: ***DORA-Anforderung:*** *Stellen Sie sicher, dass die IKT-Sicherheitsrichtlinien eine Aufgaben- u Verantwortlichkeitstrennung festlegen, um Interessenkonflikte zu vermeiden, in Übereinstimmung mit dem Modell der drei Verteidigungslinien.*

DORA-Referenz Art. 2 (2g) RTS risk mgt.:
Financial entities shall ensure that the ICT security policies referred to in paragraph 1 specify the segregation of dutie arrangements in the context of the three lines of defence model or other internal risk management and control mod as applicable, to avoid conflicts of interest;

Kommentiert [MH11]: ***DORA-Anforderung:*** *Stellen Sie sicher, dass die IKT-Sicherheitsrichtlinien führende Praktike und anwendbare Standards berücksichtigen.*

DORA-Referenz Art. 2 (2h) RTS risk mgt.:
Financial entities shall ensure that the ICT security policies referred to in paragraph 1 consider leading practices and, where applicable, standards as defined in Article 2, point (of Regulation (EU) No 1025/2012;

Anhang

Verpflichtende Dokumentationen

[Beschreibung der zu führenden Dokumentation]

Abstimmungsbeteiligte

[Beschreibung der relevanten Abstimmbeteiligten an der IKT-Richtlinie]

Kommentiert [MH12]: ***DORA-Anforderung:*** *Stellen Sie sicher, dass die IKT-Sicherheitsrichtlinien die zu führenden Dokumentationen aufführen.*

DORA-Referenz Art. 2 (2f) RTS risk mgt.:
Financial entities shall ensure that the ICT security policies referred to in paragraph 1 list the documentation to be maintained;