DIN EN ISO 19650-5:2021-03 (D)

Organisation und Digitalisierung von Informationen zu Bauwerken und Ingenieurleistungen, einschließlich Bauwerksinformationsmodellierung (BIM) - Informationsmanagement mit BIM - Teil 5: Spezifikation für Sicherheitsbelange von BIM, der digitalisierten Bauwerke und des smarten Assetmanagements (ISO 19650-5:2020); Deutsche Fassung EN ISO 19650-5:2020

Inhalt

Seite

Europäisches Vorwort 4

Vorwort 5

Einleitung 6

1 Anwendungsbereich 10

2 Normative Verweisungen 10

3 Begriffe 11

4 Ermittlung des Bedarfs an einem sicherheitsbewussten Ansatz mithilfe eines Prozesses zur Bewertung der Sensibilität 13
4.1 Durchführung eines Prozesses zur Bewertung der Sensibilität 13
4.2 Bestimmung des Umfangs der Sicherheitsrisiken 13
4.3 Ermittlung der Sensibilität der Organisation 14
4.4 Ermittlung der Sensibilitäten Dritter 14
4.5 Dokumentation des Ergebnisses der Sensibilitätsbewertung 15
4.6 Überprüfung der Sensibilitätsbewertung 15
4.7 Bestimmung des Bedarfs eines sicherheitsbewussten Ansatzes 15
4.8 Dokumentation des Ergebnisses der Umsetzung des Prozesses zur Einstufung der Sicherheit 16
4.9 Sicherheitsbewusster Ansatz erforderlich 17
4.10 Kein sicherheitsbewusster Ansatz erforderlich 17

5 Einleitung des sicherheitsbewussten Ansatzes 17
5.1 Verwaltung, Rechenschaftspflichten und Zuständigkeiten im Zusammenhang mit dem sicherheitsbewussten Ansatz 17
5.2 Beginn der Entwicklung des sicherheitsbewussten Ansatzes 19

6 Entwicklung einer Sicherheitsstrategie 19
6.1 Allgemeines 19
6.2 Bewertung der Sicherheitsrisiken 20
6.3 Entwicklung von Minderungsmaßnahmen für Sicherheitsrisiken 20
6.4 Dokumentation der Restrisiken und hinnehmbaren Sicherheitsrisiken 21
6.5 Überprüfung der Sicherheitsstrategie 21

7 Entwicklung eines Sicherheitsmanagementplans 22
7.1 Allgemeines 22
7.2 Informationsbereitstellung an Dritte 22
7.3 Logistische Sicherheit 23
7.4 Verwaltung der Rechenschaftspflichten und Zuständigkeiten in Bezug auf die Sicherheit 24
7.5 Überwachung und Prüfung 24
7.6 Überprüfung des Sicherheitsmanagementplans 24

8 Entwicklung eines Plans zum Management von Sicherheitsverstößen/-vorfällen 25
8.1 Allgemeines 25
8.2 Feststellung eines Sicherheitsverstoßes oder -vorfalls 26

8.3 Eindämmung und Wiederherstellung 26
8.4 Überprüfung nach einem Sicherheitsverstoß oder -vorfall 26

9 Zusammenarbeit mit Informationsbereitstellern 27
9.1 Zusammenarbeit außerhalb formaler Informationsbestellungen 27
9.2 In den Dokumenten der Informationsbestellung enthaltene Maßnahmen 27
9.3 Leistungsnachweis nach der Informationsbestellung 28
9.4 Ende der Informationsbestellung 28

Anhang A (informativ) Informationen zum Sicherheitskontext 29
A.1 Verstehen der potentiellen Sicherheitsprobleme 29
A.2 Sicherheitsberatung 30

Anhang B (informativ) Informationen zu Typen von personenbezogenen, physischen und technischen Sicherheitskontrollen und zum Management der Informationssicherheit 31
B.1 Personenbezogene Aspekte 31
B.2 Physische Aspekte 32
B.3 Technologische Aspekte 32
B.4 Informationssicherheit 34

Anhang C (informativ) Bewertungen bezüglich der Bereitstellung von Informationen gegenüber Dritten 36
C.1 Informationsbewertung 36
C.2 Rechtliche und gesetzlich vorgeschriebene Prozesse 37
C.3 Öffentlicher Zugang zu Informationen 37
C.4 Öffentliche Präsentationen 37

Anhang D (informativ) Vereinbarungen über die Informationsweitergabe 38

Literaturhinweise 40