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

Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) - Information management using building information modelling - Part 5: S ecurity-minded approach to information management (ISO 19650-5:2020)

Contents

Page

European foreword 4

Foreword 5

Introduction 6

1 Scope 10

2 Normative references 10

3 Termsanddefinitions 10

4 Establishing the need for a security-minded approach using a sensitivity assessment process 12
4.1 Undertaking a sensitivity assessment process 12
4.2 Understanding the range of security risks 13
4.3 Identifying organizational sensitivities 13
4.4 Establishing any third-party sensitivities 14
4.5 Recording the outcome of the sensitivity assessment 14
4.6 Reviewing the sensitivity assessment 14
4.7 Determining whether a security-minded approach is required 14
4.8 Recording the outcome of the application of the security triage process 15
4.9 Security-minded approach required 16
4.10 No security-minded approach required 16

5 Initiating the security-minded approach 16
5.1 Establishing governance, accountability and responsibility for the security- minded approach 16
5.2 Commencing the development of the security-minded approach 17

6 Developing a security strategy 18
6.1 General 18
6.2 Assessing the security risks 18
6.3 Developing security risk mitigation measures 19
6.4 Documenting residual and tolerated security risks 19
6.5 Review of the security strategy 20

7 Developing a security management plan 20
7.1 General 20
7.2 Provision of information to third parties 21
7.3 Logistical security 21
7.4 Managing accountability and responsibility for security 22
7.5 Monitoring and auditing 22
7.6 Review of the security management plan 22

8 Developing a security breach/incident management plan 23
8.1 General 23
8.2 Discovery of a security breach or incident 23

8.3 Containment and recovery 24
8.4 Review following a security breach or incident 24

9 Working with appointed parties 24
9.1 Working outside formal appointments 24
9.2 Measures contained in appointment documentation 25
9.3 Post appointment award 26
9.4 End of appointment 26

Annex A (informative) Information on the security context 27

Annex B (informative) Information on types of personnel, physical, and technical security controls and management of information security 29

Annex C (informative) Assessments relating to the provision of information to third parties 33

Annex D (informative) Information sharing agreements 35

Bibliography 37