ISO 19650-5:2020 (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: Security-minded approach to information management

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Establishing the need for a security-minded approach using a sensitivity assessment process

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

5 Initiating the security-minded approach

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

6 Developing a security strategy

- 6.1 General
- 6.2 Assessing the security risks
- 6.3 Developing security risk mitigation measures
- 6.4 Documenting residual and tolerated security risks
- 6.5 Review of the security strategy

7 Developing a security management plan

- 7.1 General
- 7.2 Provision of information to third parties
- 7.3 Logistical security
- 7.4 Managing accountability and responsibility for security
- 7.5 Monitoring and auditing
- 7.6 Review of the security management plan

8 Developing a security breach/incident management plan

- 8.1 General
- 8.2 Discovery of a security breach or incident
- 8.3 Containment and recovery
- 8.4 Review following a security breach or incident

9 Working with appointed parties

- 9.1 Working outside formal appointments

9.2 Measures contained in appointment documentation
9.3 Post appointment award
9.4 End of appointment

Annex A (informative) Information on the security context

A.1 Understanding the potential security issues
A.2 Security advice

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

B.1 Personnel aspects
B.2 Physical aspects
B.3 Technological aspects
B.4 Information security

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

C.1 Information assessment
C.2 Regulatory and statutory processes
C.3 Public access to information
C.4 Public presentations

Annex D (informative) Information sharing agreements

Page count: 28