ISO 35001:2019-11 (E)

Biorisk management for laboratories and other related organisations

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Context of the organization 7
4.1 Understanding the organization and its context 7
4.2 Understanding the needs and expectations of interested parties 8
4.3 Determining the scope of the biorisk management system 8
4.4 Biorisk management system 8

5 Leadership 8
5.1 Leadership and commitment 8
5.2 Policy 9
5.3 Roles, responsibilities, and authorities 9
5.3.1 Top management 10
5.3.2 Senior management 10
5.3.3 Biorisk management committee 10
5.3.4 Biorisk management advisor 11
5.3.5 Scientific management 11

6 Planning 12
6.1 Actions to address risks and opportunities 12
6.1.1 Hazard and/or threat identification and analysis 12
6.1.2 Risk assessment 12
6.1.3 Risk mitigation 13
6.1.4 Performance evaluation 13
6.2 Biorisk management objectives and planning to achieve them 13

7 Support 14
7.1 Resources 14
7.1.1 Worker health programme 14
7.2 Competence 15
7.2.1 Behavioural factors and worker management 15
7.2.2 Personnel reliability measures 15
7.3 Awareness 16
7.3.1 Training 16
7.4 Communication 16
7.5 Documented information 17
7.5.1 General 17
7.5.2 Creating and updating 17
7.5.3 Control of documented information 17
7.5.4 Information security 18
7.6 Non-employees 18
7.7 Personal security 18
7.8 Control of suppliers 18

8 Operation 19
8.1 Operational planning and control 19
8.2 Commissioning and decommissioning 19
8.3 Maintenance, control, calibration, certification, and validation 20
8.4 Physical security 20
8.5 Biological materials inventory 20
8.6 Good microbiological technique 20
8.7 Clothing and personal protective equipment (PPE) 20

8.8 Decontamination and waste management 20
8.9 Emergency response and contingency planning 21
8.9.1 Emergency scenarios 21
8.9.2 Emergency plan training 21
8.9.3 Emergency exercises and simulations 21
8.9.4 Contingency plans 21
8.10 Transport of biological materials 21
8.10.1 Transport security 22

9 Performance evaluation 22
9.1 Monitoring, measurement, analysis, and evaluation 22
9.2 Internal audit 22
9.3 Management review 23

10 Improvement 23
10.1 General 23
10.2 Incident, nonconformity, and corrective action 24
10.3 Continual improvement 24

Bibliography 26