INTERNATIONAL STANDARD

# ISO/IEC 27035-2

First edition
2016-11-01

# Information technology — Security techniques — Information security incident management —

## Part 2: Guidelines to plan and prepare for incident response

*Technologies de l'information — Techniques de sécurité — Gestion des incidents de sécurité de l'information —*

*Partie 2: Lignes directrices pour planifier et préparer une réponse aux incidents*

Reference number
ISO/IEC 27035-2:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

# Contents

Page

**Foreword** v

**Introduction** vi

**1 Scope** 1

**2 Normative references** 1

**3 Terms, definitions and abbreviated terms** 2
3.1 Terms and definitions 2
3.2 Abbreviated terms 2

**4 Information security incident management policy** 3
4.1 General 3
4.2 Involved parties 3
4.3 Information security incident management policy content 4

**5 Updating of information security policies** 6
5.1 General 6
5.2 Linking of policy documents 6

**6 Creating information security incident management plan** 6
6.1 General 6
6.2 Information security incident management plan built on consensus 7
6.3 Involved parties 8
6.4 Information security incident management plan content 8
6.5 Incident classification scale 12
6.6 Incident forms 12
6.7 Processes and procedures 12
6.8 Trust and confidence 13
6.9 Handling confidential or sensitive information 14

**7 Establishing an incident response team (IRT)** 14
7.1 General 14
7.2 IRT types and roles 14
7.3 IRT staff 16

**8 Establishing relationships with other organizations** 19
8.1 General 19
8.2 Relationship with other parts of the organization 19
8.3 Relationship with external interested parties 20

**9 Defining technical and other support** 20
9.1 General 20
9.2 Examples of technical support 22
9.3 Examples of other support 22

**10 Creating information security incident awareness and training** 22

**11 Testing the information security incident management plan** 24
11.1 General 24
11.2 Exercise 24
11.2.1 Defining the goal of the exercise 24
11.2.2 Defining the scope of an exercise 25
11.2.3 Conducting an exercise 25
11.3 Incident response capability monitoring 26
11.3.1 Implementing an incident response capability monitoring program 26
11.3.2 Metrics and governance of incident response capability monitoring 26

**12 Lessons learned** 27
12.1 General 27
12.2 Identifying the lessons learned 27