

ISO/IEC 27010:2015-11 (E)

Information technology - Security techniques - Information security management for inter-sector and inter-organizational communications

| Contents | | Page |
|--------------------|-------------------------------------------------------|-------------|
| Foreword | | vi |
| Introduction | | vii |
| 1 | Scope | 1 |
| 2 | Normative references | 1 |
| 3 | Terms and definitions | 1 |
| 4 | Concepts and justification | 1 |
| 4.1 | Introduction | 1 |
| 4.2 | Information sharing communities | 2 |
| 4.3 | Community management | 2 |
| 4.4 | Supporting entities | 2 |
| 4.5 | Inter-sector communication | 2 |
| 4.6 | Conformity | 3 |
| 4.7 | Communications model | 4 |
| 5 | Information security policies | 4 |
| 5.1 | Management direction for information security | 4 |
| 5.1.1 | Policies for information security | 4 |
| 5.1.2 | Review of the policies for information security | 5 |
| 6 | Organization of information security | 5 |
| 7 | Human resource security | 5 |
| 7.1 | Prior to employment | 5 |
| 7.1.1 | Screening | 5 |
| 7.1.2 | Terms and conditions of employment | 5 |
| 7.2 | During employment | 5 |
| 7.3 | Termination and change of employment | 5 |
| 8 | Asset management | 5 |
| 8.1 | Responsibility for assets | 5 |
| 8.1.1 | Inventory of assets | 5 |
| 8.1.2 | Ownership of assets | 5 |
| 8.1.3 | Acceptable use of assets | 6 |
| 8.1.4 | Return of assets | 6 |
| 8.2 | Information classification | 6 |
| 8.2.1 | Classification of information | 6 |
| 8.2.2 | Labelling of information | 6 |
| 8.2.3 | Handling of assets | 6 |
| 8.3 | Media handling | 6 |
| 8.4 | Information exchanges protection | 7 |
| 8.4.1 | Information dissemination | 7 |
| 8.4.2 | Information disclaimers | 7 |
| 8.4.3 | Information credibility | 7 |
| 8.4.4 | Information sensitivity reduction | 8 |
| 8.4.5 | Anonymous source protection | 8 |
| 8.4.6 | Anonymous recipient protection | 8 |

| | | |
|--------|----------------------------------------------------------------------|----|
| 8.4.7 | Onwards release authority | 9 |
| 9 | Access control | 9 |
| 10 | Cryptography | 9 |
| 10.1 | Cryptographic controls | 9 |
| 10.1.1 | Policy on the use of cryptographic controls | 9 |
| 10.1.2 | Key management | 9 |
| 11 | Physical and environmental security | 9 |
| 12 | Operations security | 9 |
| 12.1 | Operational procedures and responsibilities | 9 |
| 12.2 | Protection from malware | 10 |
| 12.2.1 | Controls against malware | 10 |
| 12.3 | Backup | 10 |
| 12.4 | Logging and monitoring | 10 |
| 12.4.1 | Event logging | 10 |
| 12.4.2 | Protection of log information | 10 |
| 12.4.3 | Administrator and operator logs | 10 |
| 12.4.4 | Clock synchronization | 10 |
| 12.5 | Control of operational software | 10 |
| 12.6 | Technical vulnerability management | 10 |
| 12.7 | Information systems audit considerations | 10 |
| 12.7.1 | Information systems audit controls | 10 |
| 12.7.2 | Community audit rights | 10 |
| 13 | Communications security | 11 |
| 13.1 | Network security management | 11 |
| 13.2 | Information transfer | 11 |
| 13.2.1 | Information transfer policies and procedures | 11 |
| 13.2.2 | Agreements on information transfer | 11 |
| 13.2.3 | Electronic messaging | 11 |
| 13.2.4 | Confidentiality or non-disclosure agreements | 11 |
| 14 | System acquisition, development and maintenance | 11 |
| 15 | Supplier relationships | 12 |
| 15.1 | Information security in supplier relationships | 12 |
| 15.1.1 | Information security policy for supplier relationships | 12 |
| 15.1.2 | Addressing security within supplier agreements | 12 |
| 15.1.3 | Information and communication technology supply chain | 12 |
| 15.2 | Supplier service delivery management | 12 |
| 16 | Information security incident management | 12 |
| 16.1 | Management of information security incidents and improvements | 12 |
| 16.1.1 | Responsibilities and procedures | 12 |
| 16.1.2 | Reporting information security events | 12 |
| 16.1.3 | Reporting information security weaknesses | 13 |
| 16.1.4 | Assessment of, and decision on, information security events | 13 |
| 16.1.5 | Response to information security incidents | 13 |
| 16.1.6 | Learning from information security incidents | 13 |
| 16.1.7 | Collection of evidence | 13 |
| 16.1.8 | Early warning system | 13 |
| 17 | Information security aspects of business continuity management | 13 |
| 17.1 | Information security continuity | 13 |
| 17.1.1 | Planning information security continuity | 13 |
| 17.1.2 | Implementing information security continuity | 14 |
| 17.1.3 | Verify, review and evaluate information security continuity | 14 |
| 17.2 | Redundancies | 14 |

| | | |
|------------------------------|------------------------------------------------------------------------------------|-----------|
| 18 | Compliance | 14 |
| 18.1 | Compliance with legal and contractual requirements | 14 |
| 18.1.1 | Identification of applicable legislation and contractual requirements | 14 |
| 18.1.2 | Intellectual property rights | 14 |
| 18.1.3 | Protection of records | 14 |
| 18.1.4 | Privacy and protection of personally identifiable information | 14 |
| 18.1.5 | Regulation of cryptographic controls | 14 |
| 18.1.6 | Liability to the information sharing community | 14 |
| 18.2 | Information security reviews | 15 |
| | | |
| Annex A (informative) | Sharing sensitive information | 16 |
| Annex B (informative) | Establishing trust in information exchanges | 21 |
| Annex C (informative) | TheTrafficLightProtocol | 25 |
| Annex D (informative) | Models for organizing an information sharing community | 26 |
| Bibliography | | 32 |