scriboard®
Advocates & Legal Consultants

the
IP-TECH
law series
2018

Guide to

Information Security Management System

Policy Checklist

LAW WIRE®
COMMUNICATING THE LAW™

Information Security Management System
ISO/IEC/27001

Policy Checklist

With specific regard to the new responsibilities which arise as a result of the Indian Rules recently issued under Section 43A of the IT [Amendment] Act, Chief Privacy / Security Officers, Data Protection Managers, In-House Counsels or any other officer designated by the organization for securing Information and Communications Technology [ICT] infrastructure security and operations should take strict note that their organization must comply with the International Standard IS/ISO/IEC 27001 on "Information Technology / Security Techniques / Information Security Management System" which has been prescribed by the Government of India as one of the approved Information Security Management System. Industry associations or industry cluster who are following other codes [and not IS/ISO/IEC 27001] of best practices for data protection and fulfils the preliminary requirement, must get their codes of best practices approved by the government.

Benefits of Information Security Management System

1. Business Continuity Plans
2. Business Impact Assessment
3. IT Disaster Recovery Plans
4. Information Security Incident Reports on Significant Incidents
5. Threat and Vulnerability Check
6. Compliance with legislation
7. Increased reliability and security of systems
8. Cost-effective and consistent information security
9. Systems rationalization
10. Improved management controls
11. Better human relations
12. Improved risk management and contingency planning
13. Enhanced customer and trading partner confidence
14. Information assets registry
    - Backup and Archive Register
    - Business Continuity Plan Register
    - Information Security Risk Register
    - Information Security Incident Register
    - Privilege/Administrator Access and Authorization List
    - Software License Register
    - Standard Desktop Software List
    - System Patch and Antivirus Status Register
    - Third Party Access and Connection Register

Heads under ISMS - ISO/IEC/27001 [Information Security Management System]

1. Information Security
2. Confidentiality and Non-Disclosure Agreements
3. Contact with authorities and Contact with special interest groups

4. Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities
5. Terms and Conditions for Employment in Information processing business
6. Asset Management
7. Human Resources Security
8. Physical and Environmental Security
9. Communications and Operations Management
10. Access Control
11. Information Systems Acquisition, Development and Maintenance
12. Information Security Incident Management
13. Business Continuity Management
14. Compliance with Legal Requirements
15. Training and Awareness

Policies as per various heads under ISO/IEC/27001 [ISMS]

1. Information Security
    - IT Security Policy [Information Security Management System Policy]
    - Data Security Policy
    - Sensitive Information Protection Policy
    - Data Archive and Retention Policy
    - Information Security Best Practices policy
    - Third Party Access Policy
    - Automatic Forwarded Email Policy
    - Backup and Recovery Policy
    - Anti Spam Policy
    - Anti Malware Policy
    - Access Control Policy
    - Acceptable Internet Use Policy
    - User Access Authorization Policy
    - Email Use Policy
    - Internet usage Policy
2. Confidentiality and Non-Disclosure agreements
    - Third Party Agreements Policy
3. Contact with authorities and Contact with special interest groups
    - Unauthorized Disclosure of Official Information Policy
4. Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities
    - Outsourcing and Third Party Information Policy
    - Privacy Policy
    - Spam Policy
    - Third Party Access Policy
5. Terms and Conditions for Employment in Information Processing Business
    - Personnel security Policy
6. Asset Management
    - Laptop Security Policy
    - Mobile Teleworking Policy
    - Sensitive Information Policy
7. Human Resources Security

- Change in Management Policy
- Change in Control Policy
- Delegation of Responsibility (Network & System) Policy
- Employee IT Use Policy
- Laptop Policy
- Server Policy

8. Physical and Environmental Security
   - Physical Security of Equipments Policy
   - System data backup
   - IT Security Assessment Policy
   - Environment Protection Policy
9. Communications and Operations Management
   - Email Retention Policy
   - System Usage Monitoring Policy
   - Acceptable Use of Computing Resources Policy
   - Web Content Approval Policy
   - Mass distribution of Email Policy
10. Access Control
    - Clear Screen and Clean Desk Policy
    - Password Policy
    - Wireless Network Policy
    - Wireless Access Policy
11. Information Systems Acquisition, Development, Maintenance and Disposal
    - Equipment/Devices Acquisition Policy
    - Disposal of Equipments/Devices Policy
    - Acquisition of Server Policy
    - Transfer of Server Policy
    - Maintenance of Server Policy
    - Disposal of Stored Data / Documents Policy
    - Disposal of Technology and Media Equipment
12. Information Security Incident Management
    - Risk Assessment Policy
    - Information Sensitivity Policy
    - Evidence/Reporting Policy
    - Cyber Risk Policy
    - Emergency Response Policy
    - Risk Management Policy
    - Security Breach or Suspicious Activity Policy
13. Business Continuity Management
    - Business Continuity Policy
    - Cyber Insurance Policy
14. Compliance with Legal Requirements
    - IPR Policy
    - Cyber Law Policy
15. Training and Awareness
    - Ownership, Data Management and Accountability Policy

SCRIBOARD
Advocates and Legal Consultants

www.scriboard.com

Scriboard is a full-service commercial law firm with cutting-edge specialisation in intellectual property, commercial laws, domain name disputes, data privacy / protection, technology including compliance, new media, telecommunications, legal training and allied services. Scriboard regularly advises Fortune 500 and other leading multinational and national companies on a plethora of issues.

LAWWIRE
Communicating The Law

www.lawinfowire.com

Law Wire is a platform, which focuses on providing an in depth coverage on the ever changing Intellectual Property, TMT and New Media Law sector in India and the world. Law Wire bridges the gap between legal knowledge on one hand and the legal policy making on the other. Law Wire is also a platform where readers would get an in depth knowledge of issues pertaining to Intellectual Property and Information Technology Law. This platform endeavours to provide an opportunity to lawyers [including law students] and other professionals in the legal domain to express their views and work in a collective capacity.

Copyright © 2017
All Rights Reserved
SCRIBOARD