



## **ADEC Information Security Domains & Controls**

- Security Standards & Best Practices
- Security for Human & Physical Resources
- Communications & Operations Management
- Access Control
- Information Systems Acquisition,  
Development & Maintenance
- Business Continuity Management
- Compliance

# Security Standards & Best Practices

## 1. ISO 14001:2004 CERTIFICATION

- Environmental Management System (EMS)
- Identification and Analysis of Environmental Aspects
- Establishment of Objective, Targets and Programmes
- Management and reduction of Environmental Impacts
- Compliance to Applicable Legal and Environmental Regulatory Requirements
- Certified as of December 2009

## 2. ISO 27001:2005 CERTIFICATION

- Information Security Management System (ISMS) – for the provision of Business Process Outsourcing (BPO) Services including the following IT-enabled activities: Data receipt/Downloading; Data Research; Evaluation; Analysis and Abstracting (Data Conversion/Entry and Data uploading)
- Certified as of March 2007

## 4. ISO 9001:2008 CERTIFICATION

- Quality Management System (QMS) – for the provision of Global Business Process Outsourcing Services
- Certified as of November 2005

## 5. SECURITY POLICY

- Documented Information Security Policy in place
- Documentation maintained, controlled and managed via an EDMS
- Awareness activities are conducted through new employee orientation (ISMS 101), e-learning and classroom type sessions for all new and existing employees.

## 6. ORGANIZATION OF INFORMATION SECURITY

- Information Security Manager reporting directly to the CEO
- Existence of SMCD
- Member of external organizations – BPAP, ITAP

## 7. ASSET MANAGEMENT

- Asset inventory maintenance and monitoring process via an Asset Management System
- SAM-certified (BSA) which affirms that all software are licensed
- Hardware monitoring (HAMON) & software monitoring (SOMON) systems and real-time monitoring systems for servers
- Practices information classification and labelling as per distribution, retention, disclosure and disposal
- Data destruction policies and processes existent
  - Paper disposal/crosscut shredding procedure
  - Hard drive wiping through DBAN and if hard drive is unusable, it is physically destroyed beyond re-use

# Security for Human & Physical Resources

## 1. EMPLOYMENT

### • Prior to Employment

- Background checks (criminal history, neighborhood, educational, work history, personal reference) for all new employees and contractuels
- More stringent screening process for critical positions such as Dbase and Network Admins
- Additional checks (credit) for supervisors and up and critical IT positions

### • During Employment

- Information security duties and responsibilities are enumerated in the employment contract and job description
- Employees sign confidentiality statements and non-disclosure agreements

### • Termination/Change of Employment

- Established a resign loop email account informing concerned departments of an employee resignation and corresponding revocation of logical system access (email account, usernames) and physical premise (ID card) entry

## 2. SECURE AREAS

- Compound fenced by a barb-wired perimeter wall with 24-hour on-duty security guards
- Premises monitored through CCTV System with DVR retention of 120 days
- Access level-based proximity card system
- In-house roving guards
- Color-coded ID system
- Visitors are escorted and issued color-coded ID's when inside the premises and sign NDA's whenever necessary

## 3. EQUIPMENT SECURITY

- Access Control procedure
- Bag inspections and body frisking during ingress and egress
- Temperature-controlled work areas
- Fire suppression mechanisms deployed such as extinguishers, fire/smoke detectors
- UPS and Automatic Volt Regulators (AVR) with built in surge suppressors
- Structured cabling
- Regular preventive maintenance recorded and reviewed
- No storage device drives and USB ports disabled

## Communications & Operations Management

- a. Operational Procedures and Responsibilities (Documentation, change management, segregation of duties, separation of development, test & operational facilities)
- b. Third Party Service Delivery Management
- c. System Planning & Acceptance (Capacity management)
- d. Protection against malicious & mobile code
- e. Back-up
- f. Network Security Management
- g. Media Handling (Disposal)
- h. Exchange of Information (Media in transit, electronic messaging, interconnection of systems)
- i. Electronic Commerce Services (Website hosting)
- j. Monitoring (Detection of unauthorized activities, audit logging, admin & operators logs)

## Access Control

- a. Business requirement for Access Control (Access control policy)
- b. User Access Management (Privilege management)
- c. User Responsibilities (Password selection and use)
- d. Network Access Control (External connection authentication)
- e. Operating System Access Control (Secure log-on, use of utilities, session time-out)
- f. Application & Information Access Control (Sensitive system isolation)
- g. Mobile Computing & Teleworking

## Information Systems Acquisition, Development & Maintenance

- a. Security Requirements of Information Systems
- b. Correct processing in applications (Input/output data validation)
- c. Cryptographic Controls (Key management)
- d. Security of System Files (Access to source code)
- e. Security in Development & Support Processes (Change management)
- f. Technical Vulnerability Management

# Business Continuity Management

## A. BUSINESS CONTINUITY PLANNING

- Documented Business Continuity Plan (BCP) is based from the results of a Business Impact Analysis
- BCP includes departmental procedures for critical functions that are needed when BCP is activated, a communication and escalation plan, and a list of important people, institutions and entities with corresponding contact details
- BCP is regularly tested through desktop audits, confidence tests and back-up integrity tests
- Power redundancies; UPS; multiple generator sets
- Three times redundant with Internet Service Providers with automatic switchover upon failure of primary connection

## B. INFORMATION SECURITY INCIDENT MANAGEMENT

- Documented procedures for reporting and handling IT, physical security, non-IT/ Non-security and medical incidents
- Incident reporting and data-gathering through Issue Management System
- Existence of high-level Information Security Investigation Committee (ISIC) which addresses serious IS breaches
- Incidents are consolidated for review and analysis by SMCD on a weekly, monthly and annual basis

## C. EMERGENCY RESPONSE PLANNING

- Established an Emergency Response Team
- Existing procedures for different emergency situations such as fire, severe weather, earthquake, bomb threat, etc.
- Regularly tested by conducting fire drills and evacuation exercises which are observed and documented for improvement purposes

## D. DISASTER RECOVERY PLANNING

- Has documented procedures on recovery from IT-related disasters (internet connection failure, major power breakdown, network virus outbreak, critical server crash)

# Compliance

## A. COMPLIANCE WITH LEGAL REQUIREMENTS

- Maintains a matrix of relevant and applicable laws that is reviewed and updated regularly
- Adheres to Intellectual Property Rights by prohibiting downloading and unauthorized installation of applications in workstations

## B. COMPLIANCE WITH SECURITY POLICIES & STANDARDS, AND TECHNICAL COMPLIANCE

- Documented security manual in our Electronic Document Management System (EDMS) readily accessible to authorized users (employees and third party)
- New employees have to take the ISMS 101 course as part of company induction, a module dedicated solely to Information Security within the organization
- Third parties with interest (e.g. contracted janitorial services, suppliers, service providers) are also mandated to attend ISMS 101 and sign contracts with inherent information security clauses

## WORLDWIDE LOCATIONS

### USA

10 Monument Street  
Deposit, New York 13754  
Tel.: +1 (607) 467 4600  
Fax: +1 (607) 467 4632  
Email: usa@adec-group.com

### UNITED KINGDOM

5th Floor, Hyde Park Hayes 3  
11 Millington Road  
Hayes UB3 4AZ  
Tel.: +44 (0) 845 165 6245  
Fax: +44 (0) 20 3070 0890  
Email: uk@adec-group.co.uk

### AUSTRALIA

13-15 Smith Street  
Chatswood, NSW 2067  
Tel.: +61 (02) 9418 7822  
Email: australia@adec-group.com

### SINGAPORE

20A Mosque Street  
Singapore 059500  
Tel.: +65 6532 3266  
Email: singapore@adec-group.com

### PHILIPPINES

26th Floor Philippine AXA Life Centre  
Sen. Gil Puyat Avenue  
1200 Makati City  
Tel.: +63 (2) 775 0632  
Email: philis@adec-group.com

### CHINA

Jin Yan Long Building, Suite 1608A  
Hui Long Guan, Changping district  
Beijing, 100096  
Tel.: +86 (10) 6203 1420  
Fax: +86 (10) 6238 2915  
Email: china@adec-group.com

7th Floor (701 & 702)  
25 Wang Hai Road  
Xiamen Software Park  
Xiamen, P.R. China  
Tel: +86 592 2177850 to 59  
Email: china@adec-group.com