Information Security Policy Development

Ibrahim H. Al-Mayahi and Sa'ad P. Mansoor
School of Computer Science, Bangor University, UK
Email: {almayahi@emirates.net.ae, eesa02@bangor.ac.uk}

***Abstract*—The aim of this paper is to develop a comprehensive policy for the UAE e-Government, to protect the information systems and the exchange of information between different department's employees and citizens using e-Government services. The lack of a comprehensive information security policy was identified as a major concern and barriers to developing a secure information system for e-Government. This work describes the development of comprehensive Information Security Policy, to ensure that the UAE e-Government departments, uses the same standards in every security instance. This will make it easier for different departments to integrate, and interact with citizens, and ensure that the UAE e-Government will always be able to protect the information assets in a manner that supports and is not in conflict with providing a high level of customer service.**

***Index Terms*—information security, policy, security controls, e-government**

I. Introduction

The purpose of this paper is to establish a detailed policy for the government of the UAE, for the order of protecting the information exchange and the information systems amongst the citizens and personnel of UAE while employing the e-government services. The policy would facilitate the departments of e-government in easily integrating, interacting with the citizens, and would also ascertain that the UAE e-government would always be capable of protecting the information assets at the same time as imparting high quality services to the consumers.

A gap analysis and survey was being conducted as part of this research, and the results show that there is a lack of a detailed policy for information security across the organization [1] and [2]. This was identified as the major concern that also serves as a barrier to the development of a secure information system for the e-government. Lastly, the policy developed here ensures to bring the entire management system and the organization under a single set of requirements and to ensure that they follow a unified direction towards the protection of information security. In preparation for writing the policy document a consultation was carried out in each of the relevant departments within the UAE e-Government to determine the current working practices, we then referred to ISO27001 in order to bring these into line with this standard.

Manuscript received October 1, 2013; revised December 20, 2013.

II. Organisational Security and Responsibility

To be effective, information security must be a team effort involving the participation and support of all workers in the organization who deal with information and information systems. This policy statement clarifies the responsibilities of users as well as the steps they must take to help protect the organization information and information systems.

The responsibilities implementing and monitor of information security within the organization is very important and require the establishment of several committees to deal with the security related activities, the committees can be formed as follows:

- Information security steering committee: this committee is responsible for supporting security measures, the recommended variations in the information security policy, procedures and standards, analyzing the security related incidents and approving the remedial measures.
- Information security implementation committee: this committee is responsible for monitoring the application of the information security policy, reviewing the policy on a regular basis, and proposing variations according to the technological variations and strategies, handling security related incidents and putting into place the corrective measures [3].
- Information Security Division: the administrative unit of this committee is in charge of managing and applying the databases. The control unit is responsible for monitoring security by means of frequent reviews by employing automatic and manual techniques. The site security unit monitors the environmental and physical security controls in computer and ascertains that these controls are in compliance with the approved standards and are adequate.

III. Information Transmission

The transmission of information (data) needs to be controlled and secured, the data transfer can result in information leakage and disclosure. Data can be transferred physically by courier, mail, or messengers, and can logically be transferred by phone, Fax, or network. There are different types of controls that can be implemented to achieve security of data.

A. Physical Controls

doi: 10.12720/joams.2.2.135-139

A non-disclosure and confidential information should be agreed by every party that deals with the transfer of physical data. Classified information must be secured in sealed containers or envelopes with appropriate identifications and signatures in the duration of the transfer.

B. Phone and Fax Controls

Fax and phone are not permitted to be employed for the purpose of transferring or discussing the classified information. A distinctive confidentiality agreement must be signed by the telephone operators. Appropriate answer backs must be programmed into the fax machines. Leased accessories, software and hardware, as well as the portables must be given to the personnel after having them acknowledge themselves as the possessors of the asset.

C. Printer and Photocopier Controls

In the event that a fax machine, copier, or printer malfunctions or jams while print classified information, the responsible users are not supposed to leave the machine unless every copy of the information is no longer legible or is completely removed [4].

IV. Personnel Security (HR) Policy

A. Job Definition

All the personnel must agree to the organizational security statement and must abide by its standards. They must also keep up excellent physical security by means of questioning unfamiliar individuals, not disclosing access door lock combinations/keys, protecting access keys/cards, and keeping the doors locked. Every employee must follow the security standards and policy, and must also report any assumed security violations around them to the Information Security Division. The employees must maintain the privacy of the organizational information by keeping their login Ids and passwords confidential.

B. Third Parties

Every third party should individually sign the organizational non-disclosure agreement prior to beginning their work. In the event that the current third party is working without signing the agreement, the agreement must be completed prior to continuing with the job.

C. Disciplinary Action

In the event that an employee is observed violating the published security procedures and policies, the user would additionally be subject to the disciplinary action according to the severity of the lapse as well as their past records in the context of security issues [5].

V. Logical Security & Access Management

The personnel of any organization are responsible to maintain the integrity and confidentiality of the public as well as the organizational information. They must secure the information from getting damaged, altered or lost by means of having the security standards and processes implemented, as well as by pointing out and reporting the risks and adopting appropriate measures for mitigating those risks. Access controls must be employed by the organization together with other security based initiatives in the order of protecting the availability, integrity, and confidentiality of information.

The management may revoke or restrict the privileges granted to any user; removing, copying, inspecting or changing any system resource which might likely destabilize these objectives; and adopt any supposed essential measures for the order of managing and protecting the information systems [6].

The employees who use organizational information systems are restricted to acquire invalid access to other information systems or to disrupt, alter, or damage the systems operations by any means.

User Ids and passwords are implemented with an idea that all the users acquiring access to the organizational information systems must employ a distinctive user ID and a protected password.

The management of the UAE e-government is authorized to withdraw the system privilege of any employee at any point in time in case of violation of organizational regulations by them. Any such act is restricted, which is an interference with the proper and normal operations and which negatively impacts the capability of other individuals to employ these information systems.

The workers of the UE e-government are responsible for directly reporting every violation of information security policy to the Information Security Manager as well as the Information Security Representative of their region. The employees are not supposed to compromise communications or computer system security measures, except that they are specially approved by the Information Security Manager beforehand according to a written form. The information systems of the UAE e-government are aimed at being used for corporate purposes only. Personal usage is allowed only if it does not hinder any business operation, intrude with the employees' productivity, and take up more than a petty amount of resources which could otherwise be employed for the corporate purposes [7].

All the users, at the time of login, every user must be given information reflecting the last log-in time and date. This will allow un-authorized system usage to be easily detected.

VI. Password Standards

In case any user requires sharing data stored in the computer system, they are supposed to employ mechanisms like public directories on local area network servers, shared databases, and electronic mail. Despite the fact that the user Ids are shared for purposes like electronic mail, passwords should never be revealed to or shared with others.

Sharing the password makes the valid user exposed to the responsibility for acts taken by the other party with

the concealed password. The printing and display of passwords should be suppressed, masked or obscured so that invalid parties are not capable of observing or consequently recovering them [8].

A. Administrator Responsibilities

In the event that an invalid party compromises a system, the possessors of the system should instantly modify every password on the system involved.

B. Temporary Passwords

The preliminary passwords generated by a security administrator should be authentic only for the first on-line session of the involved user. The worker should then select some other password prior to starting any work. The default passwords supplied by the vendor should be modified prior to the employment of any communication or computer systems for the life environment of UAE e-government.

VII. Operating System & Database Security

A. Operating System Hardening

All Operating Systems installations should be configured according to vendors' recommended security hardening settings. These settings should be reviewed and approved by the Security Manager and the System Administrator prior to implementation. Hardened setup should be tested prior to live installation to ensure integration with other systems and applications.

B. Use of System Utilities

The principle of least privilege (principle of minimal privilege) shall be applied to system utilities, database tools, and systems programming functions. Access privileges must be provided to the programmers which are coherent with their job roles.

C. User Authentication

Every user ID should have an associated passkey for the order of ascertaining that just the valid users may employ that user ID. Legal Notice must be added in the login screen to every system [9].

D. Patches Implementation

System Software companies normally provide periodic fixes to a security related vulnerabilities in their products. IT and Telecommunication Department Operations hold the responsibility of providing, testing these fixes, implementing them on a live system, and updating the Information Security Manager with the patches implementation.

IT operations will utilize the proper system and database scanners to ensure the system and database security vulnerabilities are detected and corrected on a timely basis. Scanners will be scheduled to run periodically and at time intervals that ensure critical systems are checked and fixed properly. Reported vulnerabilities will be fixed manually for critical machines, and can be fixed automatically for other machines that are classified as non-mission-critical.

VIII. Applications Security

User Ids should have a unique passkey for every application system in the UAE e-government for the order of ascertaining that just the valid users may employ their user Ids. The sensitive application IDs, like the administrator and super-user accounts, must be employed only on as "as per requirement" basis. Any user must not employ these user Ids as their personal accounts.

The request for user access right must be arranged by the department manager in black and white and passed on to the administration section or the security division in the order of requesting grant to the access right. In addition the access to the development environment must be restrained just to the developers and programmers. Just the users requiring access to the production system for performing their roles must be granted with it.

The standards for access control would be applied to the results of processing. All invalid access attempts to processing results would be taken as an incident which must be reported according to the approved procedures of incident management [10].

IX. Operations Management & Security

A. Microcomputers Security

Access Security: All microcomputers (workstation, desktop, laptop, pocket computers and PDA's) must be secured against un-unauthorized access using security products (built-in or third party) commensurate with the information accessed, stored, or processed. These security utilities include operating system access tools, and third party access control tools.

Physical Controls: All microcomputers must be secured against removal or theft commensurate with the value of the computer and the information that it holds. All loss or theft of microcomputers must be immediately reported according to the security incident management procedure.

Controlling Input/Output Drives and Ports: To protect UAE e-Government information from leakage to external parties, and to avoid introducing unnecessary or harmful software to UAE e-Government network, CD-ROMs, floppy drives, USB ports and other input/out ports on all user workstations should be disabled, unless explicit authorization is available to do otherwise. Any exception to this policy should be pre assessed and approved by the Information Security Manager.

Unattended Management: Remote un-attended management systems are not authorized in UAE e-Government networks unless explicit approval is obtained from the Information Security Manager. Affected users should be officially informed of the availability of such systems and the possible impact on their systems and data.

B. Virus Protection

Antivirus software should be installed and updated on every microcomputer, mail server, internet server, and LAN server attached to the network of UAE e-government. IT Support Divisions and IT Operations

should ascertain that virus signatures employed by every uninstalled instance of virus-scanning software is updated frequently. The virus detection software should be employed for scanning every file and media introduced to the UAE e-Government network. The software must not be downloaded by the users from external systems and such software must also not be introduced which is not validated by the telecommunication and IT department on to the network of UAE e-government.

C. Data Backup, Restore & Retention

For protecting the information resources of UAE e-government from being damaged or lost, the users of personal computers are in charge of frequently backing up the data on their PCs, or being certain that somebody else has done the job for them.

D. Software Licensing

The management of telecommunication and IT department should ascertain that adequate license are achieved from the vendors for every business activity. Every software should be bought by means of the Purchasing Department in collaboration with the telecommunication and IT department. The users should not copy the software imported by the UAE e-government to any storage media and transfer it to any other PC, unless the concerned IT Division Head provides an advanced permission. The software must not be installed by the users on their PCs or network servers. An appropriate Inventory Management system must be employed for performing ongoing supervision on the installed software for ensuring compliance with the license [11].

E. Information Storage & Disposal

The network and computer backup storage media should be stored in a distinct location for ensuring the accessibility of data resources in case of emergency occurrences when the data or the production machines may be accessed. The employees of the organization should not store secretive, confidential, or private information on PCs' hard drives. Disposal of sensitive information contained in the computer storage media should be carried out in a way thereby restraining the retrieval of information in future.

F. Encryption

Transfer of information by means of unencrypted mediums entails the interception risk. Thus the transmission of any confidential or restricted information across the unprotected network path must be made only when the encryption facilities installed and approved by the Telecommunication and IT Department.

G. Vulnerability Management

The vulnerability management system must be used on every mission critical system, network component, and database present in the UAE e-government network. The relevant unit must ascertain that the risks database is always kept updated. System logs are checked by the control team or the security division and it is made sure that the system is updated and scanned in accordance with the standardized schedule.

H. Internet Usage Security

Internet access would be imparted only in case of the essential requirement by the users' responsibility, and after being granted it must be employed just for corporate purposes. For the fact that the information available on the internet is not reliable, the users are prohibited to download any software from the internet. Security tools must be employed for preventing invalid downloading of files.

I. Electronic Mail Usage

E-mail accounts are allocated to and are employed by the particular UAE e-government users. In the event that a user does not check their email account for a long duration, then their mail may be forwarded to some other nominated person. The email Ids of the users should clearly imitate the name of the account owner. Internal and public categories of information can be sent by the users through email. However, in the event that any sensitive information is found being sent, then the user is prohibited to send the email outside UAE e-Government email system.

J. Web Servers & Electronic Services Security

Before being posted, the Public Relations Division should approve every change made to the Internet web pages of UAE e-government to ascertain that the entire posted material has a polished and a consistent appearance and is secured by sufficient security measures. Hyperlinks that make the UAE e-Government users navigate to external websites must be approved beforehand by the Information Security Manager. Latest programs for checking viruses should be consistently enabled on every web server after being approved by the Information Security Manager.

K. Security Incident Management

Every suspected virus infection, system intrusion, and policy violation should be reported instantly in accordance with the "Incident Reporting Procedure". Every worker should immediately report in case of any severe damage to or loss of their software or hardware. The issues should be investigated by the Information Security Representatives in the Information Security Division, who concern with every possible security incident report received by them.

X. Conclusions

A clear policy needs direction and management support. It requires commitment, supporting procedures, an appropriate technical framework within which it can be implemented, a suitable degree of authority, a means by which compliance can be checked and a legally agreed response in the event of it being violated. In this vein we have created the Information Security Policy above that could be used universally across the UAE e-Government. The policy covers all areas of relevance to information security and is generic nature so that it can be applied to the specific needs of each department within the e-Government. Applying the policy across the e-Government will facilitate greater interoperability and

exchange of information between departments without causing security weaknesses.

To ensure the policy is correctly implemented and adhered to, we have proposed that a number of committees are established to oversee the adoption process and regulate any alterations that need to be made.

The requirements set in this policy should apply to all workers in the organization who have access to Information and Information Systems no matter what their status (employee, contractor, consultant, temporary, etc.). Employees who deliberately violate this and other information security policy statements should be subject to disciplinary action in accordance with the Legal Affairs Division Policies and Procedures.

ACKNOWLEDGMENT

The authors would like to thank the UAE Ministry of Interior for supporting this research.

REFERENCES

[1] I. Al-Mayahi and S. P. Mansoor, "ISO 27001 gap analysis - case study," presented at 2012 International Conference on Security and Management (SAM '12), Las Vegas, July 16-19, 2012.
[2] I. Al-Mayahi and S. P. Mansoor, "Information security culture assessment: Case study," presented at IEEE Third International Conference on Information Science and Technology (ICIST 2013), Yangzhou, China, March 27-28, 2013.
[3] Abu Dhabi Government,"Information security policy," Abu Dhabi Systems and Information Center, pp. 19-20, May 2013.
[4] R. Baskerville and M. Siponen, "An information security meta-policy for emerging organizations," *Logistic Information Management Journal*, vol. 15, no. 5/6, pp. 337-346, 2002.
[5] T. Carlson, "Information security management: Understanding ISO 17799," *International Network Services*, October 2001.
[6] G. Dhillon and J. Backhouse, "Information system security management in the new millennium," *Communications of the ACM*, vol. 43, no. 7, pp. 125-127, July 2000.
[7] T. Mikko and O. Harri, "A review of information security issues and respective research contributions," *ACM SIGMIS Database*, vol. 38, no. 1, pp. 60-80, February 2007.
[8] M. Ungerman, "Creating and enforcing an effective information security policy," *Information Systems Audit and Control Association*, vol. 6, 2005.
[9] M. Whitman and H. Mattord, *Management of Information Security*, Cengage Learning, 2010, pp. 111-118.
[10] B. Williams, *Information Security Policy Development For Compliance: ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2.0, and AUP V5.0*, CRS Press, 2010, pp. 25-29.
[11] A. Zuccato, "Holistic security management framework applied in electronic commerce," *Computers & Security Journal*, vol. 26, no. 3, pp. 256-265, May 2007.

Ibrahim Humaid Al-Mayahi, is an Engineer in the Ministry of Interior UAE, has BSc Electronic Engineering and MSc Information Security UK. His research interest is in the areas of data breaches, e-government information frameworks and information security systems.

Sa'ad Mansoor was appointed to the academic staff of the School of Computer Science at Bangor University in 2003. His research interest lies mainly in the modelling of computer networks and information security. His research has been performed in close collaboration with academic and industrial research groups.

