IT Security (Policy Document)

Issued by : Head, Information Technology and Knowledge Management (ITKM)

Purpose : This IT Security Policy applies to all IT related activities in M.Kumarasamy College of Engineering.

Scope : The document contains definitions about IT Security, guidelines and implications of security.

Reference :

1. National Cyber Security Policy and
2. Information Security Policy issued by Ministry of Electronics and Information Technology
3. Information security management system standard - ISO 27001:2005
4. Information security management system guideline – ISO 27002:2005
5. Security risk assessment – ISO 27005:2008
6. Business continuity management strategy – BS 25999-1:2006
7. Contingency planning guide for IT systems – NIST SP 800-34
8. ICT Disaster recovery process standard – ISO 24762:2008
9. Security incident management process – ISO/IEC TR 18044

1. IT Security :

1.1 Security relates to the protection of valuable assets against loss, misuse, disclosure or damage. In this context, "valuable assets" are the information recorded on, processed by, stored in, shared by, transmitted or retrieved from an electronic medium. The information must be protected against harm from threats leading to different types of vulnerabilities such as loss, inaccessibility, alteration or wrongful disclosure. Threats include errors and omissions, fraud, accidents and intentional damage. Protection arises from a layered series of technological and non-technological safeguards such as physical security measures, background checks, user identifiers, passwords, smart cards, biometrics and firewalls. These safeguards would address both threats and vulnerabilities in a balanced manner.

1.2 To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation, the IT Security Policy is defined in MKCE.

1.3 ITKM would Carry out periodic IT security risk assessments and determine acceptable level of risks, consistent with criticality of institutional functional requirements, likely impact on functions/operations and achievement of institutional goals/objectives.

1.4 ITKM would Periodically test and evaluate the adequacy and effectiveness of technical security control measures implemented for IT systems and networks. Especially, Test and evaluation may become necessary after each significant change to the IT applications/systems/networks and can include, as appropriate the following:

- Penetration Testing (announced/unannounced) - Vulnerability Assessment
- Application Security Testing
- Web Security Testing

1.5 ITKM will carry out Audit of Information infrastructure on an annual basis and when there is major upgradation/change in the Information Technology Infrastructure, by either inhouse Audit team or an independent IT Security Auditing organization

2. Security Assurance : 2.1 With security assurance, ITKM is not intending to make the system 'hacker proof', but devise a mechanism which can, to a large extent

- Anticipate potential problems
- Pre-empt through proactive measures
- Protect against considerable damages
- Ensure recovery and restoration

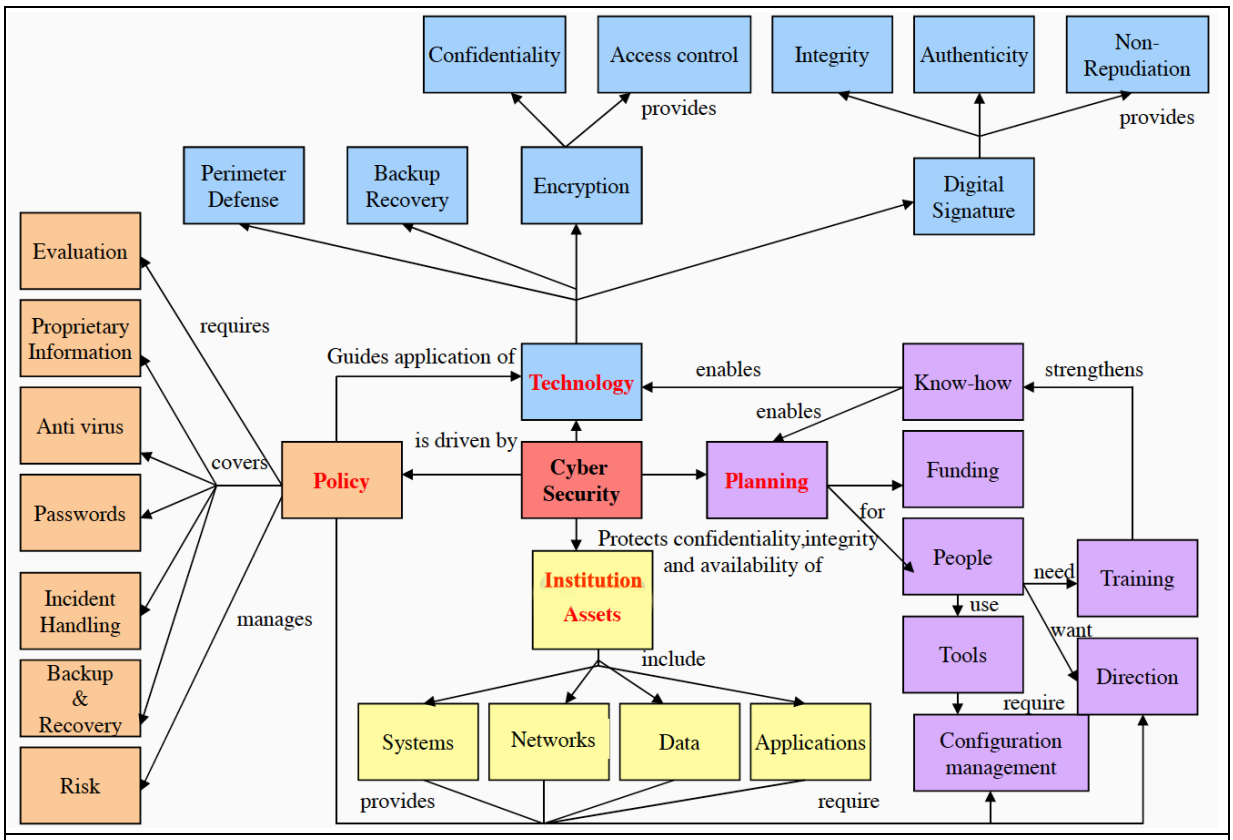

Fig. 1 Cyber Security Assurance

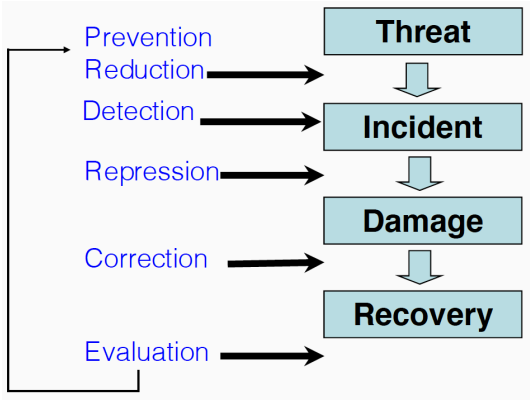

Fig. 2 Security Issue Management

2.2 Website and all web applications will be security audited.

2.3 The Security Audit would be done every six months or as and when any changes are done to the source code.

2.4 Use of SSL Certificate Site wide on all websites. The SSL Certificate would use at least 2048 bit SHA 256 encryption or higher.

2.5 Ensure that the SSL Certificate is valid and keep track of the certificate expiry date and take necessary action to renew/replace the certificate before expiry.

2.6 Disable support for SSL 2.0, SSL3.0, TLS 1.0 at the server level. Use TLS 1.2

2.7 Disable weak ciphers like DES, 3DES, RC4. Use Strong Ciphers like AES, GCM.

2.8 Any "non-https" requests received on the website/applications, would be forcefully re-directed to "https".

2.9 Ensure that all Websites and Applications and their respective CMS (Content Management System), 3rd party plugins, codes...etc., are updated to the latest versions.

2.10 All Passwords, connection strings, tokens, keys...etc., would be encrypted with salted hash. There would not be any plain passwords stored in config files or source code or in database.

2.11 All exceptions would be handled appropriately. Custom error pages would be displayed for any errors/exceptions. At no point of time, a portion of source code would be displayed on the page in case of an error or exception.

2.12 HTTP Response Headers would be obscured.

2.13 Directory traversal would be disabled. In case of any specific attempt by a user to access a portion of the code by typing the url path (ex: www.mkce.ac.in/js/custom.js) then the same would be redirected to a custom error page.

2.14 Http only Cookies would be enabled, to restrict access to cookies.

2.15 All default user names and IIS/apache pages (like admin, default.aspx, index.aspx...etc) would be renamed. The access url for admin panel/CMS, would also be renamed.

2.16 The Web Server processes would not be running under Administrator or Root user Account. A dedicated User account with limited privileges would be used for the Web Server Processes.

2.17 All websites/Applications, would be checked by their respective developers on a daily basis and in case of any security compromise, then the same would be reported to ITKM immediately.

2.18 Write + Execute Permission - both would not be given to upload directory

2.19 Ensure Input Validation is done properly, while accepting input from the user through the website.

2.20 Ensure that the Computer/system, from where CMS/site updates are being done is installed with the latest OS + Antivirus Updates and Patches. No unauthorized software/cracks, would be installed on the machine.

2.21 Restrict the web application to run Stored Procedures, so that SQL Injection attempts are averted.

2.22 If any website/application is integrated with any 3rd party Applications or using any APIs for external communication, then ensure that all such communications are done through encrypted channel.

3. Security Software used in MKCE : 3.1 ITKM recommends usage of the following Antivirus & Firewall System

No	Hardware / Software Name	License Type
1	Antivirus: Windows Defender	Purchased License (Part of Windows OS)
2	Windows Firewall	Purchased License (Part of Windows OS)
3	Antivirus: Clam AV	Open Source License Windows OS, GNU/Linux and Mac OS
4	Linux Firewall	UFW/ iptables (Part of Linux OS)
5	Cyberoam	Purchased Next-Generation Firewall for Enterprise Networks CR1500iNG–XP

3.2 ITKM recommends alertness at the Individual, Institutional and National Level and immediately report of any incidents mentioned below; so that appropriate steps can be taken without much cause to damage.

Individual Level	Institutional Level	National Level (will be reported to Govt. Authorities)
o Social Engineering o Email hacking & misuse o Cyber stalking o Identity theft & o Phishing o Financial scams o Abuse through emails o Abuse through Social o Networking sites o Laptop theft	o Website intrusion/defacement o Malicious Code o Scanning and probing o DNS server attacks o Denial of Service & o Distributed Denial of o Service o Targeted attacks o Phishing o Data theft o Insider threats o Financial frauds	o Cyber-crime & terrorism o Attacks on Critical Infrastructure o Web defacements o Website intrusion and malware propagation o Malicious Code & spread of botnets o Scanning and probing for Cyber espionage o Denial of Service & o Distributed Denial of o Service attacks o Supply chain integrity o Technical & legal inability for positive attack attribution

3.3 ITKM would as and when required use the CERT Security guidelines for its IT systems.

No	Item	Reference Policy
1	Security for Web Servers	CERT-In Security Guidelines CISG-2004-04
2	Security for Database Servers	CERT-In Security Guidelines CISG-2005-01
3	Security for Intrusion Detection Systems	CERT-In Security Guidelines
4	Security for emails	CERT-In Security Guidelines CISG-2011-01
5	Security for Wireless Access Points / Routers	CERT-In Security Guidelines CISG-2011-03
6	Security for Standalone /Networked Computers	CERT-In Security Guidelines CISG-2005-03

Dr. John Blesswin A

(Head - ITKM)

Annexure – 1

Next-Generation Firewall for Enterprise Networks CR1500iNG–XP

Cyberoam Next-Generation Firewalls (NGFW) with Layer 8 Identity-based technology offer actionable intelligence and controls to enterprises that allow complete security controls over L2- L8 for their future-ready security. Cyberoam's Human Layer 8 acts like a standard abstract layer that binds with real Layers 2-7, enabling organizations to regain lost security controls. Cyberoam CR1500iNG-XP offers inline application inspection and control, website filtering, HTTPS inspection, Intrusion Prevention System, VPN (IPSec and SSL) and granular bandwidth controls. Additional security features like WAF, Gateway AntiVirus, Anti-Spam are also available. The FleXi Ports (XP) available in CR1500iNG-XP appliances offer flexible network connectivity with I/O slots that allow additional Copper 1G, Fiber 1G/10G ports on the same security appliance.

Cyberoam security appliances offer high performance, assured Security, Connectivity and Productivity and an Extensible Security Architecture (ESA) for future-ready security in enterprises. Cyberoam NGFWs assure Security, Connectivity, Productivity