د مخابراتو اومعلوماتی ټکنالوجی وزارت

وزارت مخابرات و تکنالوژی معلوماتی

Ministry of Communications and IT - MCIT

د افغانستان اسلامی جمهوریت

جمهوری اسلامی افغانستان

Islamic Republic of Afghanistan

Ministry of Communication and IT

E-Government Directorate

E-Government Resource Center

DRAFT CYBERSECURITY PLAN

December 05, 2015

TABLE OF CONTENTS

ABBREVIATION:

1. Active Directory(AD)
2. Afghan(AF)
3. Afghanistan Cyber Emergency Response Team(AFCERT)
4. Application(AP)
5. Authentication and Authentication Accounting(AAA)
6. Certified Information Security Manager (CISM)
7. Certified Information Systems Security Professional(CISSP)
8. Demilitarized Zone(DMZ)
9. Department of Finance (DOF)
10. Domain Name Server(DNS)
11. Dynamic Host Configuration Protocol(DHCP)
12. Full disk encryption (FDE)
13. Government Islamic Republic of Afghanistan(GIRoA)
14. Information and Communication Technology(ICT)
15. Information System Security Directorate(ISSD)
16. International Multi-Lateral Partnership Against Cyber Treat(IMPACT)
17. Internet Information Service (IIS)
18. Internet Service Provider(ISP)
19. Intrusion Detection Systems(IDS)
20. Intrusion Prevention Systems(IPS)
21. Leveraged Procurement Agreement Exemption Request (LPAER)
22. Ministry of Communication and Information Technology (MCIT)
23. National Internet Exchange of Afghanistan(NIXA)
24. National internet Registry of Afghanistan(NIRA)
25. Network Operation Center(NOC)
26. Organizational Unit(OU)
27. Pre Shared Key(PSK)
28. Public Key Infrastructure(PKI)
29. Registered and Authorized Employee's (RAE)
30. Registered Jack(RJ)
31. Remote Authentication Dial in User Service(RADIUS)
32. Software Procurement Plan(SPP)

1. INTRODUCTION

The use of Information and Communication Technologies (ICT) has been spreading rapidly in Afghanistan and ICT is playing important role in all aspects of our lives. Growing need for technology in every field has expanded the spectrum of cyber-security & cyber-crime, it's emerging at a greater pace with rapidly changing advancements .The vulnerabilities inherent in ICTs may cause in high scale economic losses, information theft, illegal access and disturbance of public order and/or threats to national security. It is a fact that cyberspace offers opportunities for attackers on information systems and critical infrastructures.

As per recent Norton anti-virus report the cybercrime cost around 110 $ billion dollars worldwide, affecting 556 million victims per year with 1.5 million adult victims everyday that's 18 victims per second. Cybercrime cases are drastically increasing in Afghanistan on average Afghanistan Cyber Emergency Response Team (AFCERT) which is first responder for all cyber incidents in Afghanistan receives an average of 200 cases every month, According to survey by Kaspersky Afghanistan is marked 7th in terms of personal infection level and it is reported that 57.46 % percent of personal data of computer user is infected. Cyber Criminals exploit organizational and technical faults and vulnerabilities of the internet, the absence of a harmonized legal framework between countries, and the lack of effective coordination between national law-enforcement agencies makes the environment for criminals exceptionally conducive: minimum risks, wide coverage, and lucrative profits. The tools and knowledge required for attacks are often cheap and easy to get, and it has been observed that anyone or any systems across the world can participate in cyber-attacks, either knowingly or unknowingly. And it is deemed almost impossible to determine who finances and organizes these enduring and advanced cyber-attacks that target the information systems and critical infrastructures.

On the other side, Cyber security is evolving alongside with cybercrime and is been regularly updated to ensure they are in line with cybercrime. Securing information, services, systems and networks requires ensuring availability, integrity and confidentiality of resources. Securing network consist of physical security, network security, awareness, vulnerability assessment, administrative and human firewall. By definition "cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access, or cybersecurity refers to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals". To mitigate cyber-crime and pave the way for secure and resilient cyberspace for public and

government sector it is important to have cyber laws in place, Cyber Emergency wing, international collaboration and affiliation by establishing Network Operation Centers (NOC), awareness and capacity building. Ensuring cybersecurity requires coordinated efforts throughout an information system. MCIT needs to consider these Elements of cybersecurity as below.

- Application security.
- Information security.
- Network security.
- Disaster recovery / business continuity.
- End-user education.

2. BACKGROUND

In 2009, MCIT established the first Cyber Emergency Response Team (CERT) in Afghanistan and it was officially named as AFCERT. The mandate of AFCERT was to fight against cyber threats and crimes and provide awareness and solutions on cyber security to the government and private sector. In order to fight the said crimes, it was vital to conduct a risk assessment of all government & public ICT infrastructures and come up with a solution to mitigate those risks. All need to protect our critical information, infrastructures, as risks are huge, The rapid growth of ICTs and societal inter-dependency have led a shift to perception of Critical Information Infrastructure threats and, as a consequence, cyber security has become international agenda. It is crucial to understand the risks that accompany new technologies in order to maximize the benefits. Growing threats to security, at the level of the individual, the firms, government and critical infrastructures, make security everyone's responsibility. It is important to understand and keep up-to-date contours of fast changing challenges.

Cyberspace – the interdependent network of information technology components that supports many of our communications is a crucial component of National critical infrastructure. A secure cyberspace is critical to the health of the economy and to the security of any Nation. Developing a framework for cyber security is the need of the hour in order to address the recent and alarming rise in online fraud, identity theft, and misuse of information online.

In 2012 the first awareness workshop on drafting the National Cyber security Strategy of Afghanistan (NCSA) was held in Information and Communication Technology Institute (ICTI) .It was a four days' workshop and all government CIOs, ICT heads, private sector and academia participated and studied and analyzed various strategies from different

countries.

The NCSA committee was chaired by Information Systems Security Directorate of MCIT and held its regular meetings and assessments for one year. After a series of assessments and recommendations, the NCSA committee finalized and submitted the first draft of the strategy in July 2014 to the MCIT and ICT Council to review and adapt its action plan. We will make the cyber security plan through the National Cybersecurity strategy of Afghanistan in the inside procedure and policies of MCIT. Cybercrime and electronic transaction law was drafted under Information System and security directorate(ISSD) and soon we are going to have these laws in place, Public key infrastructure is much needed to ensure security and integrity of data communication, The security of systems is dependent on the people that use them , it is important to have cyber security awareness programs , Security awareness training can be performed in a variety of ways that can be utilized alone or in conjunction with each other. Those mediums can consist of a more thorough classroom style training, creation of a security-awareness website, pushing helpful hints onto computers when they start up and/or e-mailing helpful hints on a weekly or monthly basis, and utilizing visual aids like posters or interactive animations.

3. MCIT INVENTORY

In order to deploy security policies, devices, best practices and cyber security plan it is mandatory to have strong network ICT infrastructure in place. Technically, security is a layer on top of well-established network groundwork therefore we have done assessment of existing ICT inventory of MCIT and we proposed a model network below in Section 4 of this document below in order to lay foundation for cyber security. Table below indicates existing network inventory of Ministry of Communication and IT, It is divided into servers, switches, routers, monitors , racks, power backup, firewall , software's and accessories.

Obsolete	Active	Obsolete	Not working
Extremely low Performance	Ready to use	low performance	Need to repair

EXISTING HARDWARE INVENTORY OF MCIT					
Servers					
Sr.No	Description	Model	QTY	Active/ Not Active	Status
1	Dell Power Edge	2900	2	In use	Obsolete
2	Dell Power Edge	SC1430	3	Not in use	Obsolete
3	Dell Power Edge	2900	1	Not in use	Obsolete
4	Dell Power Edge	2800	2	Not in use	Obsolete
5	Dell OptiPlex	9010	1	In use	Active

Table 1

Switches					
Sr.No	Description	Model	QTY	Active/ Not Active	Status
1	Cisco CSKX-NM-1G(Fiber Switch)	CSKX-NM-1G	1	Active	Active
2	Cisco Catalyst Switch	2950	2	Active	Obsolete
3	Patch panels	N/A	5	Active	Active
4	Cisco Catalyst	4507R Core Fiber Switches		Active	Obsolete
5	Cisco Catalyst Switch	2960	17	Active	Obsolete

Table 2

Routers					
Sr.No	Description	Model	QTY	Active/ Not Active	Status
1	Cisco 1800 Series	1800 Series	1	N/A	Active

2	Cisco 3600 Series	3600Series	1	N/A	Active

Table3

Monitors					
Sr.No	Description	Model	QTY	Active/ Not Active	Status
1	Rack Monitor	N/A	2	Not Active	Not working
2	Dell Monitors	N/A	6	Active	Active
3	Dell Monitors	N/A	2	Not Active	Not working

Table 4

Racks					
Sr.No	Description	Model	QTY	Active/ Not Active	Status
1	Racks	N/A	4	Active	Active

Table 5

Power Back up					
Sr.No	Description	Model	QTY	Active/ Not Active	Status
1	APC	10 KVA	4	Active/ 5 minute backup)	Obsolete
2	NetPro	3000VA	1	Active/ 5 minute backup)	Obsolete
3	Power stabilizer Watford control	5000VA	4	Active	*Active*

Table 6

Firewall					
Sr.No	Description	Model	QTY	Active/ Not Active	Status

1	Juniper Net screan50	Version 50.00 or 80/Hardware screen version 4010(0)	1	Active	Obsolete

Table 7

Accessories					
Sr.No	Description	Model	QTY	Active/ Not Active	Status
r1	Network repair tool box	N/A	N/A	N/A	Not available
2	Smoke/Fire Detector's	N/A	N/A	N/A	Not available
3	Emergency lights	N/A	N/A	N/A	Not available
4	AC	Carrier Samsung	2	Active but not self-power one	Active

Table 8

MCIT EXISTING SOFTWARE INVENTORY					
Sr.No	Description	Model	QTY	Active/ Not Active	Status
1	Windows server 2003	2003	1	Not Active	N/A
2	Kaspersky	2014	500 user's	Active	Active

Table 9

4. GRAPHICAL DESIGN OF MCIT NETWORKS

4.1 CURRENT DESIGN

Graphical diagram below in figure (1) is an existing network design of Ministry of Communication and IT (MCIT), as it clearly depicts there are a lots of things missing that are required for standard network, currently there is just a basic connectivity of devices to central switch and firewall playing a small role in segmenting and assigning privileges to different categories of users. as shows in figure (1) Fiber optic terminates into fiber switch from there it goes to external interface of firewall and internal interface of firewall connects to core switch where all users of MCIT are connected, there are no specialized servers e.g., active directory, file server, print server, anti-virus server, no

Intrusion prevention/detection system (IDS/IPS), no authentication of users connecting to wireless access point and no security policies. Therefore we proposed a model solution in figure (2)

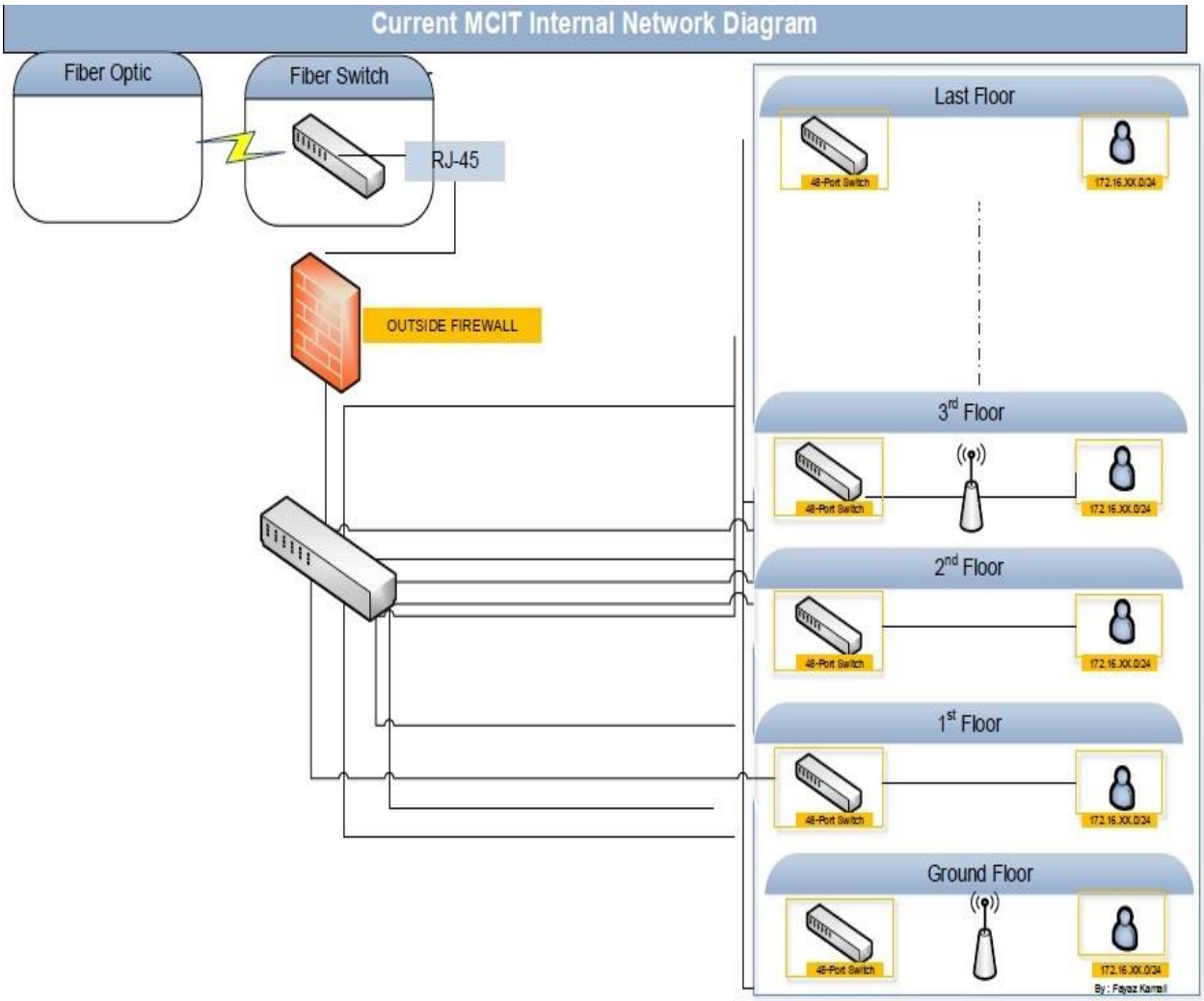


Figure 1

4.2. MCIT PROPOSED NETWORK DESIGN

The model we proposed has all the necessary components that are required for standard Network ICT infrastructure, every organization use's devices as per their rules and requirements therefore it is required to explain how these devices should be configured and designed. Each section of this diagram is explained below.

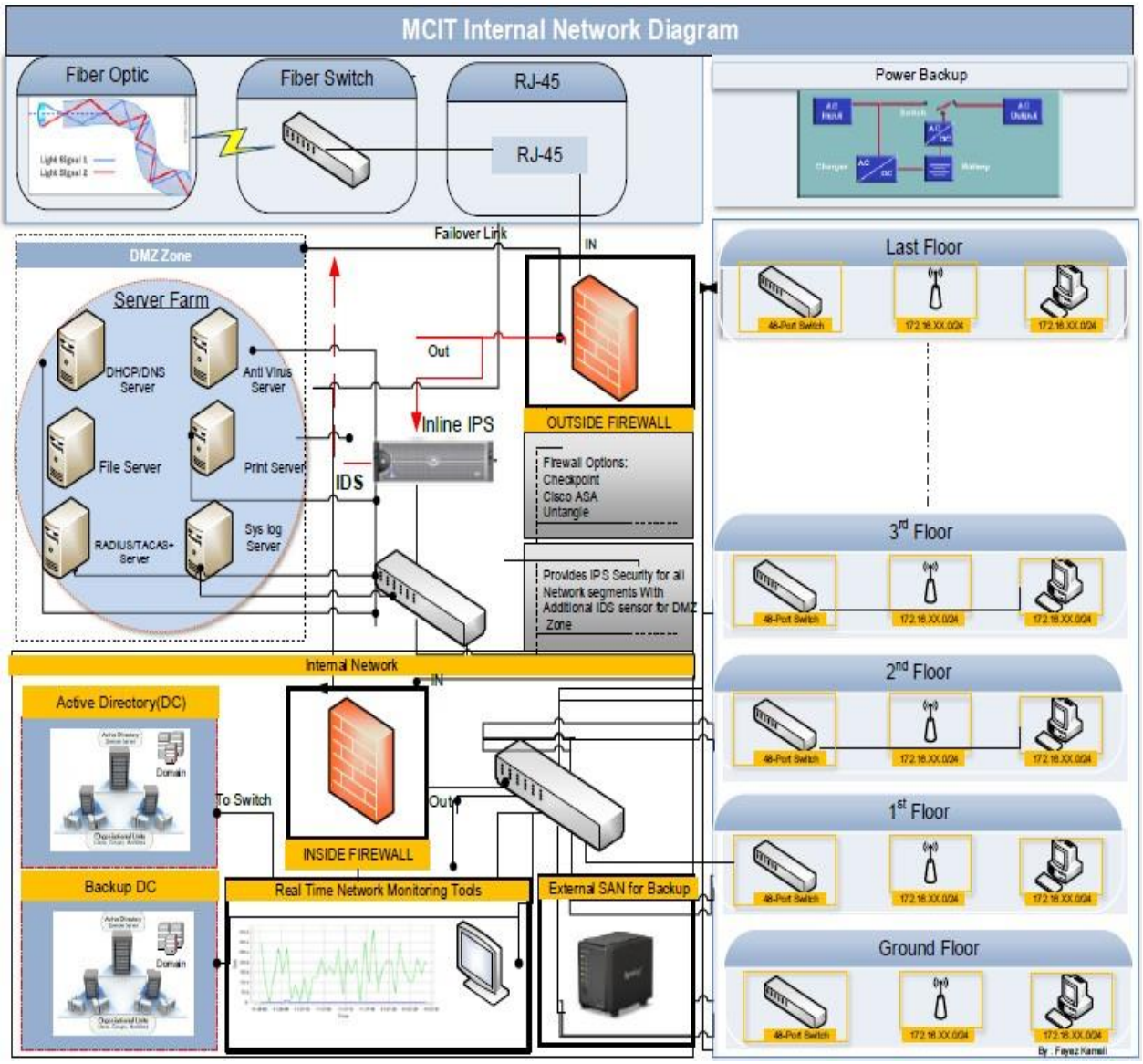


Figure 2

4.2.1: Fiber to Registered Jack (RJ) RJ- 45.

As per diagram we are getting a fiber link from Afghan Telecom to a cisco fiber switch & then to an outside firewall.

4.2.2: Outside firewall.

As shown above, RJ-45 coming from the cisco fiber switch will go to our firewall outside Zone Interface (IN) & will mark that as an insecure interface, OUT interface will connect with Intrusion Prevention Systems (IPS) to check for anomalies or suspicious traffic pattern. We deployed Intrusion Detection Systems (IDS) at Demilitarized Zone (DMZ) zone to analyze & report for any malicious traffic.

4.2.3: Server Farm.

All server farms are located at the DMZ zone which can be publically accessed. Remote users will be limited to DMZ zones & if there is any policy violation our security devices will inform & log malicious access by using IDS/IPS sensors

4.2.4: Switch

Here in our topology switch is a centralized point where all our devices are connected. We have one switch in our outside network & one at inside.

4.2.5: Inside Firewall

In the model both firewalls are in active/failover state which means if incase one goes down other will take the role, to reduce load on one device & to segment internal & external network for better security measure's we deployed two firewalls (inside, outside). The outside firewall will protect our network from the internet or outside attacks, and the inside firewall is responsible for protecting internal network.

4.2.6: Anti-Virus Server

As per figure (2) all clients will connect with anti-virus server to upgrade their local signature databases and to download any available patches of anti-virus server.

4.2.7: Active Directory & Backup

All Organizational Units (OU) & policy will be deployed in active directory, each user in departments will be authenticated & will be given privileges as per their role. An Active Directory (AD) domain controller authenticates and authorizes all users and computers in a windows domain type network assigning and enforcing security policies for all computers and installing or updating software.

4.2.8: Demilitarize Military Zone (DMZ)

In figure (2) we proposed the general idea of putting your public faced servers in the "DMZ network" so you can separate them from your private, trusted network. The use case is that because your server has a public face, it can be remotely rooted. If that happens, and a malicious party gains access to your server, he should be isolated in the DMZ network and not have direct access to the private hosts.

4.2.9: Intrusion Detection System (IDS)

We are deploying IDS System in our model to monitor malicious activities and identify any suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. IDSs can respond to the suspicious event in one of the several ways, which includes displaying an alert, logging the event or even paging an administrator.

4.2.10: Intrusion Prevention System (IPS)

The model we recommended will be deploying IPS System. IPS will monitor traffic coming from the Outside interface of the firewall; it provides policies and rules for network traffic along with IDS for an alerting system to suspicious traffic but allows the administrator to provide the action upon being alerted.

4.2.11: Domain Name Server (DNS)/ Dynamic Host Configuration Protocol (DHCP) Server

We will dedicate single server providing both Domain Name Server (DNS) &Dynamic Host Configuration Protocol (DHCP) services. All security issues considering DNS/DHCP spoofing are taken into consideration.

4.2.12: File Server

To have mobility & to minimize file sharing using external storage mediums it is recommended to have dedicated file server. Each unit on file server will have its reserved disk space with different privilege access levels.

4.2.13: Wireless Access

To have roaming wireless service throughout MCIT, we need to have several Access points (AP) installed on different floors with single Source Set Identifier (SSID) & roaming capability.

4.2.14: Remote Authentication Dial in User Service (RADIUS)

To have secure communications we can use either Remote Authentication Dial in User Service (RADUS) or Tacas+, these are an authentication and accounting system which checks that the information is correct and then authorizes access to the client. It enhanced reporting and Tracking based on source & destinations.

Scenario

When a user authenticates to an SSID using 802.1X, that individual session is encrypted uniquely between the user and access point. This means that another user connected to the same SSID cannot sniff the traffic and acquire information because they will have a different encryption key for their connection. With a Pre shared Key (PSK) network, every device connected to the access point is on a “shared encryption" connection so they can all see each other's traffic if they choose to do so. If you need to de-auto a particular user or device, having RADIUS makes this much easier because you disconnect a single user or device without having to change the key for everyone or allow that potential

security risk of that user rejoining the network with the known access key.

4.2.15: Print Server

To minimize resource usage, it is suggested to have single laser printer per floor will be accessible by all members on the same floor.

4.2.16: Syslog Server

To have full control over the network, it is recommended to have organized Logs for major applications/activities. Syslog can be used to integrate log data from many, different types of systems into a central repository. This will help us to investigate if in case something happens.

4.2.17: Switch Security Policy

As per Appendix B4.

4.2.18: Router Security Policy

As per Appendix B4.

4.2.19: Firewall policy

As per Appendix B1.

4.2.20 Information Technology Security policy

As per Appendix B2.

4.2.21 Acceptable use policy

As per Appendix B3.

4.2.22 Security recommendation for desktop computers

As per Appendix B5.

5. TRAINING PLAN FOR STAFFING & TRAINING

The weakest link in an organization's IT security plan is often its own employees. Using social engineering, malicious emails, phishing, and other tactics, criminals are often able to trick employees into disclosing private information or bringing malware inside an organization. Cyber security & awareness training strengthens security program by teaching employees about current criminal tactics so that staff can avoid them. Cyber security training can help address these issues and minimize cyber security risks. Technology is evolving at greater pace on both side of cyber criminals and cyber security, To mitigate cyber-crimes; security experts has to think ahead of criminals and should be in-line with latest tools, threats & global cyber security challenges. We have identified specific cyber security trainings that will enable security experts to be aware of latest security threats and mitigation techniques.

We will divide the training into two parts. The first part will be some sort of cybersecurity certifications another part will be cybersecurity general training it is already started, and discussed each of them in the following.

We will target the following government employees in both section of the trainings (cybersecurity general training and cybersecurity certifications)

- IT Directors of Government agencies
- Head of IT Departments in Government agencies
- IT General Managers in Government agencies
- IT Officers in Government agencies

5.2 CYBERSECURITY TRAINING

EGRC-II has plans to train 480 employees from all Government ministries and independent directorates in cyber security till December 2017 so far EGRC-II has trained 100 participants including 38 percent of females out of total contract value for 180 government employees for ongoing session.

RFP for next session of 300 cyber security employees for government employees is supposed to be advertised in March 2016 and will continue until final value of 480 employees in cyber security till 2017.

Modules	
1.(Network Security): • Firewalls • Routers • Switches • Load Balancers • Proxies • Web security gateways • VPN concentrators • NIDS and NIPS • Protocol analyzers • Spam filter • UTM security appliances • Web application firewall vs • network firewall • Application aware devices **2.(Compliance and Operational Security):** • Control types • False positives False negatives • Importance of policies in reducing risk • Riske calculation • Quantitative vs qualitative • Vulnerabilities • Threat vectors	• Adware • Virus ,Spyware **3.(Threats and Vulnerabilities):** **(Application, Data and Host Security):** • Explain the importance of application security controls and techniques. • Logic bomb Botnets Trojan Rootkits • Ransomware Polymorphic malware Armored virus **4.(Access Control and Identity Management):** • Compare and contrast the function and purpose of authentication services. • Given a scenario, select the appropriate authentication, authorization or access control. • Install and configure security controls when performing account management, based on best practices. **5.(Cryptography):** • Given a scenario, utilize general cryptography concepts & methods. • Given a scenario, use appropriate PKI, certificate management and associated components.

• Probability / threat likelihood	

Table 10

5.1 CYBER SECURITY CERTIFICATIONS

We recommend below certifications that are necessary for cyber security experts, and technical employees. Since we already have trainees who got general cyber security trainings and they have basic cyber security foundations covered already, The certifications we proposed are for high end security expert therefore we suggest to recommend top grade trainee's for certifications plan. Below modules in table 10 are covered in cyber security trainings by EGRC-II project.

Table 11

S.No	Certification	Duration	Tools/Skills Required	Description
1.	CompTIA SECURITY+	45 Hours	Workstation, Virtual Machines, Packet Tracer. Certified Instructor	A basic entry level certification for the security newcomer. It introduces the candidate to many of the security concepts and touches on many basics.
2.	CISM–Certified Information Security Manager	90 Hours	Workstation, Security Best Practices Manual, Certified Instructor.	A business oriented certification focusing on management, design and risk. It is the Information Security professional's gateway to understanding the broad concepts of information assurance and ultimately securing it, serves security managers, business security architects amongst others.
3.	CISSP-Certified Information Systems Security Professional	90 Hours	Workstation, Security Best Practices Manual, Certified Instructor.	Composed of 10 knowledge domains in various security topics ranging from physical security to management. The CISSP is more technically oriented and relates to some of the more complex topics like cryptography, network security, authentication and authorization, serves the security analyst.
4.	LPT-Licensed Penetration Tester	60 Hours	Kali Linux, Back track, Windows Server, Workstation, Workbook, Test PC's. Certified Instructor	EC-council has restructured how this certification is attained and this requires in addition to achieving the CEH and ECSA a practical exam, a must for the dedicated penetration tester.
5.	CEH-Certified Ethical Hacking	60 Hours	Kali Linux, Back track, Windows Server, Work station, Workbook, Test PC's. Certified Instructor	A highly regarded certification in industry mainly focus on offensive security, explains security exploitation and vulnerability analysis best practices using Kali or back track.
6.	Cisco-Certified Network Associate (CCNP)-Security	60 Hours	Packet Tracer, GNS3 simulator, 2 Routers 3XXX Series, 4 switches, Firewall, IPS/IDS, ISE. Certified instructor.	Professional Level Cisco certifications, covering IPS, IDS, VPN, Firewall, ISE, AAA and other security modules.

6. CYBERSECURITY AWARENESS PLAN

The security of systems is dependent on the people that use them. One of the greatest threats to information security could actually come from within company or organization, Inside 'attacks' have been noted to be some of the most dangerous since these people are already quite familiar with the infrastructure. It is not always unhappy workers and corporate spies who are a threat. Often, it is the non-malicious, uninformed employee's. Cyber security awareness focus will be on uninformed users who can do harm to your network by visiting websites infected with malware, responding to phishing e-mails, storing their login information in an unsecured location, or even giving out sensitive information over the phone when exposed to social engineering. Some of the more important items to cover in your security awareness training are your organization's security policy, data classification and handling, workspace and desktop/laptop security, wireless networks, password security, phishing, hoaxes, malware, file sharing and social engineering.

Security awareness training is an important necessity for any organization. If the user base is properly informed as to what to watch for, prevention, and remediation procedures, this alone could prevent a lot of potential problems that could affect the infrastructure and the company as a whole. Often it is just awareness that is the key to prevention and protection.

Security awareness training can be performed in a variety of ways that can be utilized alone or in conjunction with each other. Those mediums can consist of a more thorough classroom style training, creation of a security-awareness website, pushing helpful hints onto computers when they start up and/or e-mailing helpful hints on a weekly or monthly basis, and utilizing visual aids like posters.

6.1. SECURITY AWARENESS WEBSITE

Another way of implementing a security awareness program is through the creation of a security awareness website. Information system and security directorate (ISSD) should come up with website which could consist of different sections with the different areas that need to be covered, another implementation of the security awareness website could be a self-paced tutorial where users can log in and go through it, taking mini quizzes at the end of each section to make sure the material is actually being read and absorbed. Utilizing logins can also be a means of keeping track of who has (and more importantly who has not) taken the training.

6.1.1. Helpful Hints

Utilizing helpful hints and tips is more of a supplement to the training, be it via classroom style or online, Helpful hints can consist of tips and reminders that are pushed to user screens when they log in. These tips and reminders can consist of key points emphasized in the training (e.g. “Never keep your password in a place that can be accessed or viewed by anyone besides yourself.”). Reminders can be as simple as reminding someone to change their password or run their virus scan.

6.1.2. CLASSROOM-STYLE TRAINING

Utilizing a classroom setting for security-awareness training can offer the benefit of lecture-based and interactive learning as well as the availability of someone to answer questions in real time. There can also be a Q&A period after the materials are presented as well as contact information distributed for questions that might pop up afterward.

6.1.3. Animated Ads

Animated Security awareness short movies. The Awareness team should come up with short informative animated movies on cyber awareness & its mitigations. Such animated movies have to be broadcast on all platform’s to cover maximum audience.

6.2. SOCIAL MEDIA

Using Facebook and twitter to launch awareness of cyber-related issues and activities.

6.2.1. YouTube Channel:

Cyber security Official YouTube channel which will have technical reviews by ICT professional regarding cyber security threats in Afghanistan. Awareness campaigns or any informative documentaries related to technology. Customize videos will be made in local languages on best practices of technology use e.g. smart cards/ATM usage/online banking etc…

6.2.2. Official Forum/Blog for ICT Professional Articles

Official blogging sites will be published for open discussion on any cyber related issues. Brainstorming sessions on this forum/blog will be arranged to improve cyber security activities in Afghanistan to get best ideas from professionals in the related field. Awareness team needs to bring together more ICT professionals to this forum in regular base to keep the forum updated.

6.3. BROADCAST MEDIA

6.3.1. Radio Channels

Short documentaries/scenario's on Cyber security awareness & its impact on the community. Short advertisement's regarding day to day technology crime awareness.

6.4. NEWSPAPER

Detail reports of any major cyber security incident to local newspapers in Afghanistan.

6.5. PUBLIC AWARENESS

Cyber Awareness Seminar's to public and private institutions. The team will target the universities, corporate sector, schools/colleges, leading Internet Service Providers (ISP), private sector, and government's organizations.

6.6. IMPACT & ISSD

To get real-time monitoring, MCIT, AFCERT NOC has been operational at the earliest & it will be connected with IMPACT Malaysia as soon as possible to get better reporting on cyber threats in Afghanistan.

7. CYBER SECURITY THREATS

Now that we have addressed possible methods in implementing security awareness. Training, what should be covered in the training will be addressed. These topics will help employees understand why security awareness is important and guide them in knowing how to prevent incidents from happening and what to do if one occurs.

7.1. PHYSICAL SECURITY

When addressing physical security, locking your doors and desk/file cabinet drawers. Should be the main focus. A helpful item to include could be the crime statistics, more specifically thefts, from the organization. Another item to lightly touch upon (but go into greater detail in Desktop Security) is the fact that if a potential attacker has access to a user's computer, they could install a key logger or actually get into a machine that has not been locked.

7.2. DESKTOP SECURITY

The desktop security section should go into detail as to why it is important to either have a password-protected screen saver or, even better, to get into the habit of locking computers when users walk away from them. A screensaver timeout should be utilized so if a user walks away from their computer, the password-protected

screensaver would come up. Tactics a potential attacker could utilize (e.g. Shoulder surfing, key loggers, etc.) also need to be addressed

7.3. WIRELESS NETWORKS SECURITY

The wireless networks and security section should address the unsecure nature of
Wireless networks as well as tips and tricks to exercise caution and harden laptops against the dangers of 'sniffing.' Emphasis should also be placed on not storing any kind of sensitive information on laptops that will be accessing a wireless network. Another area that should be covered is the importance of firewalls. Windows Firewalls by themselves are not enough. Most times companies will provide a purchased firewall on company-supplied laptops and computers but personal laptops that may utilize the company wireless network need to have a firewall on them.

7.4. PASSWORD SECURITY

The password security section should include what constitutes a strong, secure password with an emphasis on passphrases since they are harder to guess and to crack. This section should also outline the minimum password requirements of the organization. Sharing passwords as well as leaving them out where anyone but the user could access them should be strongly discouraged. Making this part of organization-wide policy could be very helpful in this arena. If this is incorporated into policy, this should be addressed in the training. Users need to be aware a policy is in place and general "rules of thumb" to make sure these policies are followed.

7.5. PHISHING

When discussing phishing, the term as well as the purpose should always be defined. Examples are key to this portion of security awareness training. Things to avoid (e.g. Clicking on links provided in e-mail, submitting banking and password information via email, etc.) should be highly emphasized so people know what to look for.

7.6 HOAXES

Hoaxes should be addressed in the training because a lot of time and resources can be spent reading and forwarding hoax emails. The types of hoaxes as well as examples should be the meat of this section. Using familiar hoaxes is the best option so it will be easier to grasp. It could also be beneficial to compare hoaxes to viruses in that they are spread by continually forwarding them. The dangers of hoaxes should also be addressed because some hoaxes warn of a virus and tell users to delete valid and sometimes important system files.

7.7 MALWARE

When addressing malware, it should always be defined and then broken down into its categories: viruses, worms, Trojans, spyware, and adware. After each category is broken down, address how they end up on systems.

7.8 VIRUSES

Start out by outlining what makes a virus. It is important for users to be able to identify a potential virus when they see one or to identify characteristics of a virus that has already infiltrated the user's system. What a virus is capable of is also something that should supplement the defining of what makes a virus what it is?

7.9 WORMS

The worms section can be handled much the same way the virus section is handled

Definition, how to spot, what it is capable of, how to prevent, what to do If one invades the system.

7.10 MAN-IN-THE-MIDDLE ATTACKS.

Access to network packets that come across the networks is phrased as man-in-middle attacks. These attack can result in information theft, control over an ongoing session to gain access to one's internal network resources, traffic analysis to derive information network and its users, denial of service, corruption.

7.11 TROJANS

Trojans portion should define what they are, what they can do, what can be done to prevent them, and what to do in the event of one making it onto the system

7.12 Spyware and Adware

Again, spyware and adware should be defined, what they can do should be outlined, prevention tips and tricks, and then what to do if it is found on the system. Spyware and adware identification and removal programs should also be addressed, most of which are free (e.g. Ad Aware, Spy Sweeper, etc.).

7.13. MALVERTISING

One of the growing issues of the past year is "malvertising "the implantation of malicious advertisements onto websites.

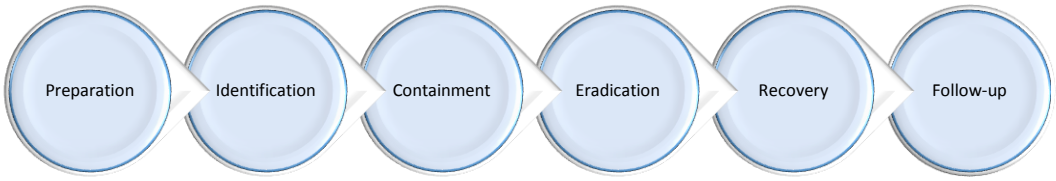
7.14. SOCIAL ENGINEERING TECHNIQUES ON SOCIAL NETWORKS

Training should cover Social engineering tricks used to persuade people to undermine their own online security. This can include opening an email attachment, clicking a button, following a link, or filling in a form with sensitive personal.

8. SOFTWARE PROCUREMENT PLAN

9. INCIDENT RESPONSE PLAN

In an incident response process, it is very important for the Cyber Emergency Response Team (CERT) to mitigate the incident as soon as possible to minimize loss of data and resources. The process should follow a proper guideline that is developed based on a well-defined incident response framework (as illustrated in Figure 3 below). The



Figure(3)

framework, which comprises six phases ensure a consistent and systematic approach in handling such incidents. Each of the phases is elaborated in detail in Section 5 of this procedure. This systematic approach will enable AFCERT team to handle any cyber security related incident in a proper and standard way. Cybercrime has no boundaries it is spread across continents therefore it is necessary to have affiliation with

International cybercrime groups like IMPACT (*International multilateral partnership against cyber threats*) which has growing members from several countries. By becoming a member of international group's MCIT will be able to use that platform to address any cyber security incident across the border.

9.2. OBJECTIVE

This document outlines systematic approach for the Afghanistan Cyber Emergency Response Team (AfCERT) in handling security-related incident.

9.3. SCOPE

The primary audience of this document includes all AfCERT and others who may participate in preparation, identification, containment, eradication, recovery and follow-up efforts.

9.4. DEFINITIONS[1]

Security-related incident	*Any adverse event that threatens the security of information resources, including disruption or loss of confidentiality, integrity, or availability of data. Adverse events include, but are not limited to, attempts (successful or persistent) to gain unauthorized access to an information system or its data; unwanted disruption or denial of service; unauthorized use of a system; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. Examples include insertion of malicious code (for example, viruses, Trojan horses, or back doors), unauthorized scans or probes, successful or persistent attempts at intrusion, and insider attacks.*

Constituency	A specific group of people and/or organizations that have specific services offered by AfCERT.
AfCERT	An acronym for Afghanistan Cyber Emergency Response Team. This is a team providing services to a defined constituency.

[1] The definitions are derived from Incident Prevention, Warning, and Response (IPWAR) Manual, USDOE, 205.1-1, Sep 2004 and also Handbook for Computer Security Incident Response Teams (CSIRT), 2nd Edition, and April 2003.

9.5. PROCEDURE

Chart below explains the workflow for the incident response process in detail.

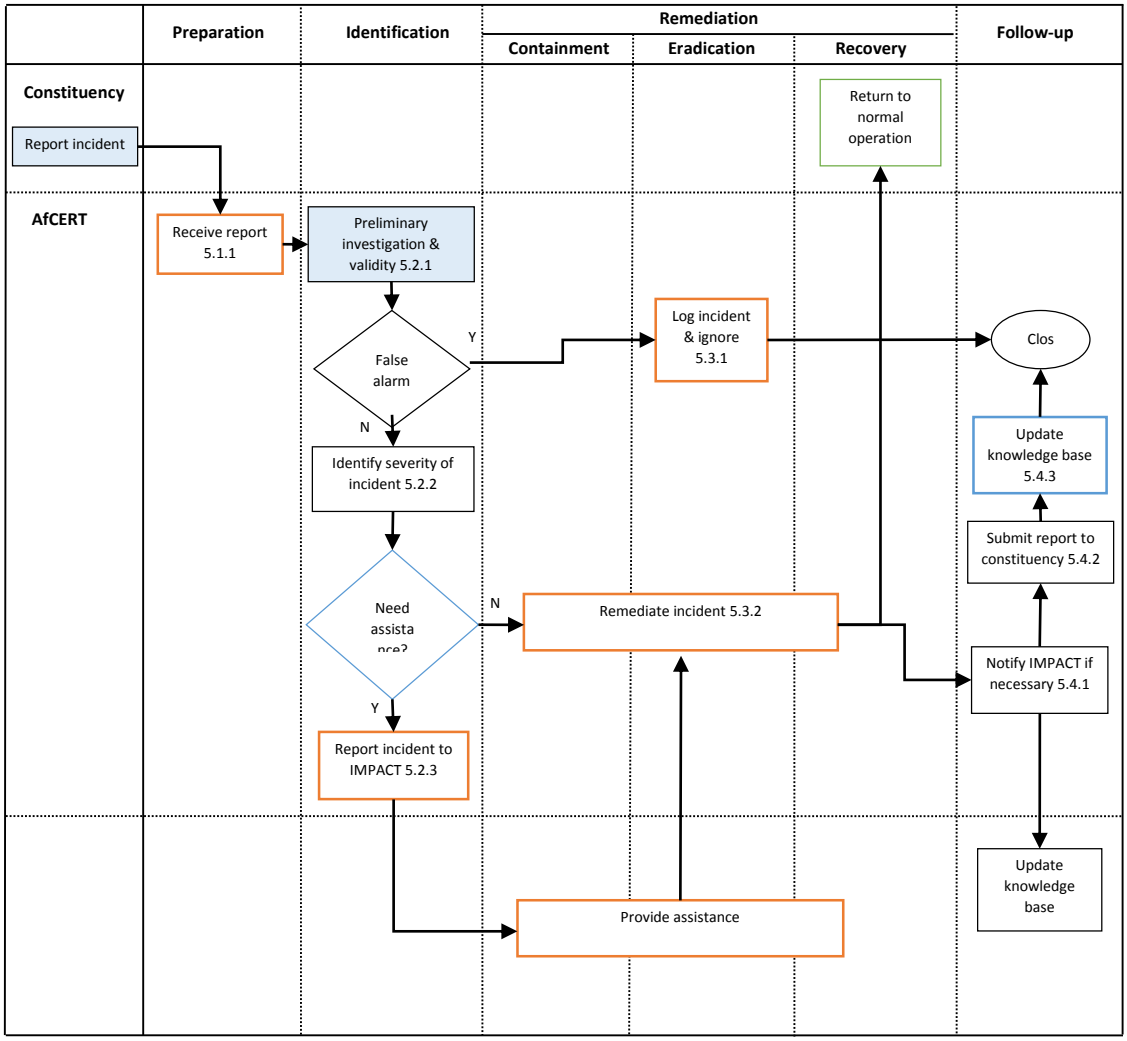


Figure (4) AfCERT incident response workflow

9.5.1 Preparation

9.5.1.1 Receive report

This is the preliminary phase of the incident handling process, during which the incident shall be reported to the AfCERT. The incident shall be able to be reported via various means; AfCERT's portal, email, phone, fax or other means necessary.

The report received shall include a description of the incident and as much of the following information as possible; however, subsequent actions should not be delayed in order to gain additional information:

- Name of reporting agency/partner
- Point of contact information including name, telephone, and email address
- Incident date and time, including time zone
- Source IP, port, and protocol
- Destination IP, port, and protocol
- Operating System, including version, patches, etc.
- System Function (e.g., DNS/web server, workstation, etc.)
- Antivirus software installed, including version, and latest updates
- Location of the system(s) involved in the incident
- Method used to identify the incident (e.g., firewall, IDS, IPS, audit log analysis, system administrator)

The information provided by constituency shall be used to fill up the AfCERT Incident Reporting Form as attached in Appendix A1. A unique incident number must be assigned to each case. Depending on the criticality of the incident, it may not be always feasible for the reporting agency/partner to gather all the information prior to reporting. In this case, the team shall continue with the next step of the incident response process as further information is being collected.

9.5.2 Identification

9.5.2.1 Preliminary investigation & validity

When an incident is reported, preliminary investigation shall be conducted to determine the validity of the incident. During this process, the team has to determine whether it is a real incident or just a false alarm. False alarm can be triggered by many events such as system misconfiguration, ISP service interruption, network component failure and so on.

If a valid incident is reported, Section 5.2.2 is followed in order to identify the severity of the incident. If it is a false alarm, Section 5.3.1 is followed to dismiss the alarm.

9.5.2.2 Identify severity of incident

Once it is confirmed that the incident is valid, the severity level of the incident shall be determined. The severity identification will assist to determine the necessary actions that should be performed to remediate the incident.

The team can classify the incident severity by considering the affected users of the system, and also the classification of information at risk due to the incident. Some of the question that can be asked to assist the team in determining the severity are listed in the AfCERT Incident Reporting form. Determining the level of severity shall be conducted by referring to the Table () below:

Severity level	Low	Medium	High
Impact	• Loss of system confidentiality, integrity, and availability. • Expected to have a limited effect on the operations, assets, or individuals.	• Loss of system confidentiality, integrity, and availability. • Expected to cause major damage on the operations, assets, or individuals.	• Loss of system confidentiality, integrity, and availability. • Expected to cause loss or severe damage to the operations, assets, or individuals.
Activities	• Monitoring activity of services that threaten the information and resources	• Interception of critical communication • Disruption of non-critical services • Unauthorized access and usage of information and resources	• Unauthorized disclosure, modification or deletion of sensitive information • Disruption of critical services
Information escalation	• AfCERT	• AfCERT and higher authority	• AfCERT and higher authority
Maximum response time	• 72 hours	• 48 hours	• 24 hours

Table 1: Incident severity and response time

9.5.2.3 Report incident to IMPACT

If the team needs assistance in resolving the incident, a report can be made to the Global Response Centre (GRC) of IMPACT to request for assistance in the remediation process.

The team can use the GRC portal to report the incident or by other means necessary; email, fax, or phone.

9.5.3 Remediation

9.5.3.1 Log incident & ignore.

During the event where the reported incident is conformed to be a false alarm, the team shall log the incident and ignore the incident. The affected constituency shall be informed about the closure of the reported incident.

9.5.3.2 Remediate incident

In order to remediate the incident, the team is generally responsible to assist and/or to advice its constituency to:

- Isolate the system.
- Monitor the incident.
- Warn the relevant constituencies affected by the incident and providing emergency instructions to them.
- Report to relevant law enforcement agencies if necessary.
- Request additional resources from IMPACT or other relevant agencies.

The team shall decide whether it has the capacity and capability to resolve the incident on its own or seek assistance from IMPACT. If the team needs assistance, a report shall be made to IMPACT by any available communication channels such as GRC portal, phone, email or fax.

The team shall escalate the recommendations and suggestions to the reporting constituency to remediate the incident. The team shall ensure that the constituency is able to resume to its normal operation. Relatively simple incidents, such as attempted but unsuccessful intrusions into systems, require only assurance that the incident did not in any way affect system software or data stored on the system. Complex incidents, such as malicious code planted by insiders, may require a complete restore operation from clean backups or a complete reinstall of the operating system and software applications. It is essential to verify a restore operation was successful and that the system is back to a normal condition.

9.5.4 Follow-up

9.5.4.1 Notify IMPACT if necessary

Information on any part of the incident response process can be escalated to IMPACT if the team believes that the information will benefit other parties around the world. The team shall decide the extent of information disclosure prior to releasing the information to IMPACT. The information shall only be shared after removing organization-specific and country-specific information.

9.5.4.2 Submit report to constituency

An incident report shall be created and disseminated to constituency at the end of the incident response exercise. Some of the elements that can be considered to be included in the report are as follows:

- A description of the exact sequence of events
- The type and severity of incidents
- Remediation measure put in place
- Assessment to determine if the remediation steps taken are sufficient
- Recommendations need to be considered for improvement

The report shall be reviewed by management prior to releasing it to the affected constituency. This is to ensure the document is properly prepared and contain sufficient information needed by the constituency.

9.5.4.3 Update knowledge base

Once the reporting constituency resumes its normal operation, the team shall update the knowledge base. Among other things to update are details on the incident, how it was remediate and also lessons learnt, to improve on the identified areas and used as reference for future incidents.

Depending on the confidentiality agreement with the constituency, some information may be removed before updating them into the knowledge base.

9.6. ADVISORY TO CONSTITUENCY

One of the important roles of AfCERT is to provide threat advisory to its constituencies. The team shall follow the workflow depicted in Figure 5 below in order to disseminate threat advisories:

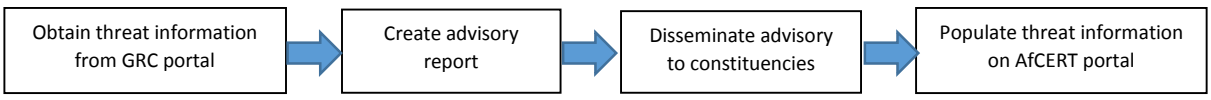


Figure (5): AfCERT advisory dissemination workflow

9.6.1 Obtain threat information from GRC of IMPACT

In order to provide advisories to its constituencies, AfCERT shall routinely review threat information from GRC portal of IMPACT.

9.6.2 Create advisory report

Once the advisories are obtained, the team shall use the information obtained from GRC portal to create an advisory report for its constituencies. The advisory report shall be created by filling up the AfCERT Advisory Template in Appendix A2. The sample of the AfCERT Advisory can be referred in Appendix A3.

9.6.3 Disseminate advisory to constituencies

Once the advisory report is completed, AfCERT shall disseminate the report to its constituencies via email communication.

9.6.4 Populate threat information on AfCERT portal

The threat information can also be made available to its constituency and the general public by uploading the information on the AfCERT portal.

9.7 DOCUMENTATION

All details related to the incident response process shall be documented and filed for trackback and easy reference. This provides valuable information to unravel the course of events and can serve as evidence if prosecution of intruders is necessary. It is recommended that the following items be maintained:

- System events (log records)
- Summary of incident (including how the incident occurred, category, severity and origin of the incident)
- Incident response action taken (including the time that an action is performed)
- Communication with all external parties (including person with whom the discussion was held, the date and time and the content of the communication)

10. PUBLIC KEY INFRASTRUCTURE IMPLEMENTATION PLAN

PKI (Public Key Infrastructure) has been recognized as a key element for supporting secure and reliable electronic communications in the framework of e-government and e-service delivery. Several countries have implemented, or are in the process of implementing PKI for internal purposes. PKI might be seen as a prerequisite for implementing electronic support for internal administrative procedures as well as a prerequisite for electronic service delivery to

citizens and businesses. Particularly when we are talking about E-government & E-services, PKI would be playing an integral part to provide secure electronic communication.

Setting up a PKI that suits MCIT security goals involves making numerous decisions, PKI seems to offer a coherent and efficient security solution to authentication and other security challenges when communicating electronically however the complex nature of PKI and rapid technology development pace render it quite challenging for government policy makers to make right decisions about its implementation and use.

MCIT has existing PKI infrastructure in place, all what is required to do is to provide trainings, PKI use policies, technical operational support & maintenance to initiate PKI. In order to establish a national policy on the management of PKI in the government many issues needs to be addressed, such as:

- Cross-border interoperability with other governments
- Public access issues related to the use of PKI for e-services to citizens and businesses
- Information management issues related to digitally signed documents and retention over time
- Interoperability testing of PKIs, certificates, certificate directories
- Rules for the use of PKI for confidentiality purposes
- Technical specifications for government PKI – standards
- Market policies (government use of the PKI-market)
- Management of a large scale rollout of PKI.

Following are what a properly designed and implemented PKI achieves:

10.2. CONFIDENTIALITY

A PKI implementation ensures confidentiality of data transmitted over the network between two parties. Data is protected through the encryption of messages, so even in cases where the data is intercepted; the data would not be able to be interpreted.

10.3. AUTHENTICATION

The PKI also provides the means by which the sender of the data messages and the recipient of the data messages can authenticate the identity of each other. Digital certificates which contain encrypted hashes are used in authentication, and to provide integrity.

10.4. INTEGRITY

Integrity of data is assured when data has been transmitted over the network, and have not modified in any manner. With PKI, any modification made to the original data, can be identified.

10.5. NON-REPUDIATION

In PKI, non-repudiation basically means that the sender of data cannot at a later stage deny sending the message. Digital signatures are used to associate senders to messages. The digital signature ensures that the senders of messages always sign their messages. This basically means that a particular person cannot, at a later stage, deny sending the message.

10.6. PKI DEPLOYMENT ISSUES AND CONSIDERATIONS

Since MCIT has PKI infrastructure in place following are the standard steps required to deploy, maintain and operate Public Key Infrastructure (PKI).

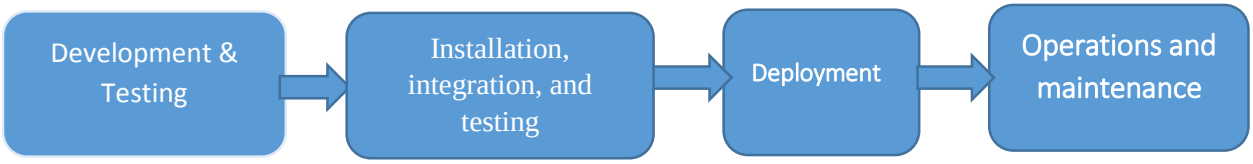


Figure (6)

Table (12)

Step 1	**Development and testing**	Development and testing focuses on testing all software's and system components. This takes place before your PKI is installed. Development and testing involves: • developing and testing customized PKI components • documenting your organization's PKI operations manual • enhancing your facilities (if required) • Training PKI operations staff, registration authorities, and helpdesk staff

Step 2	**Installation, integration, and testing**	In this phase MCIT should installs all components of the PKI. All operations are closely monitored. Installation, integration, and testing involves • installing network, firewall, hardware, operating system, and third-party devices and components. • installing supporting Directory and Web software • installing Entrust software and supporting hardware • integrating back-end systems • testing all functionality
Step 3	**Deployment**	Deployment involves running your PKI in a pilot program, followed by full rollout. Deployment consists of: • engaging the pilot user community • running the pilot for short time • monitoring PKI usage and feedback • monitoring operations staff, registration authorities, helpdesk staff, and performance • enhancing the PKI environment as required • initiating full rollout
Step 4	**Operations and maintenance**	With active deployment complete and PKI usage under way, MCIT must ensure continued operation and maintenance. Operations and maintenance involves: • conducting ongoing maintenance and support services. • Trainings and capacity building of employees.

11. PLAN FOR IMPLEMENTING DATA AT REST ENCRYPTION TO PROTECT DATA

11.2 NEED FOR ENCRYPTION

The purpose of data at rest encryption is to understand storage encryption technologies for end user devices and in planning, implementing, and maintaining storage encryption solutions. The types of end user devices addressed in this plan are personal computers (desktops and laptops), consumer devices (e.g., personal digital assistants, smart phones), and removable storage media (e.g., USB flash drives, memory cards, external hard drives, writeable CDs

and DVDs). This section provides practical, real-world guidance for three classes of storage encryption techniques: full disk encryption, volume and virtual disk encryption, and file/folder encryption. Businesses today need tools to protect against the known threats and to guard against as yet unknown threats. Effective threat and vulnerability management must be proactive rather than reactive, preventing problems rather than responding to them. Encrypting “data at rest” is a key element when addressing these concerns.

11.3. ENCRYPTION CONCEPT

Encryption transforms data that is unprotected, or plain text, into encrypted data, or ciphertext, by using a key. Without knowledge of the encryption key, the ciphertext cannot be converted back to plain text

11.4. ENCRYPTION CHALLENGES

Encryption, as described previously, depends on encryption keys. Those keys must be, at the
same time, kept secure and available, and responsibilities must be split:

11.4.1 Key security

To preserve the security of encryption keys, the implementation must be such that no one
Individual (person or system) has access to all of the information that is required to determine the encryption key.

11.4.2 Key availability

More than one individual (person or system) has access to any single piece of information necessary to determine the encryption key. In a system-based solution, redundancy is provided by having multiple isolated key servers. In addition, backups of the key server’s data are maintained.

11.4.3 Separation of responsibilities

To prevent one person from gaining access to the data, the handling of a recovery key requires at least two people with the role of Security Administrator. This ensures that one person cannot access the data, and it also ensures separation between the Security Administrator and Storage Administrator roles.

11.5. STORAGE ENCRYPTION TECHNOLOGIES

There are many technologies available for encrypting data stored on end user devices. We are going to describe the most commonly used technologies for data at rest encryption , it discusses the protection provided by each type, and explains how these technologies are typically managed.

11.6. COMMON TYPES OF STORAGE ENCRYPTION TECHNOLOGIES

We have explained a high-level overview of the most commonly used options for encrypting stored information: *full disk encryption*, *volume and virtual disk encryption, and file/folder encryption*. Below is brief summary of different types of encryptions.

11.6.1 Full Disk Encryption

Full disk encryption (FDE) or whole disk encryption will encrypt all the data on the hard drive used to boot a computer, including the computer's OS, and permitting access to the data only after successful authentication. This kind of encryption will help secure all data in hard drive.

11.6.2 Virtual Disk Encryption and Volume Encryption

Virtual disk encryption which can hold many files and folders, and permitting access to the data within the container only after proper authentication is provided, at which point the container is typically mounted as a virtual disk. Virtual disk encryption is used on all types of end user device storage. The container is a single file that resides within a logical volume. Examples of volumes are boot, system, and data volumes on a personal computer, and a USB flash drive formatted with a single filesystem. *Volume encryption* is the process of encrypting an entire logical volume and permitting access to the data on the volume only after proper authentication is provided. Volume encryption is most often performed on hard drive data volumes and volume-based removable media, such as USB flash drives and external hard drives.

11.6.3 File/Folder Encryption

File encryption is the process of encrypting individual files on a storage medium and permitting access to the encrypted data only after proper authentication is provided. Folder encryption is very similar to file encryption, only it addresses individual folders instead of files. Although folder encryption and virtual disk encryption sound similar—both a folder and a container are intended to contain and protect multiple files—there is a difference. A container is a single opaque file, meaning that no one can see what files or folders are inside the container until the container is decrypted. File/folder encryption is transparent, meaning that anyone with access to the file system can view the names and possibly other data for the encrypted files and folders, including files and folders within encrypted folders, if they are not protected through OS access control features. File/folder encryption is used on all types of storage for end user devices. File/folder encryption can be implemented in many ways, including through drivers, services, and applications. When a user attempts to open an encrypted file (either encrypted by itself or located in

an encrypted folder), the software requires the user to first authenticate successfully. Once that has been done, the software will automatically decrypt the chosen file. Because it decrypts a single file at a time, the performance impact of file/folder encryption should be minimal. File/folder encryption is most commonly used on user data files, such as word processing documents and spreadsheets.

12. Timeline for National Cyber Security Plan[1]

NO	Action	Responsible and Relevant Entity	Supporting Organization	Deadline	Remarks
1.	Draft Cybercrime Law	MCIT, ISSD, MoJ, Parliament	US-DOC, CLDP, Council of Europe, IMPACT, UNCITRAL	December 2016	Cybercrime Law was already drafted, EGRC-II is only responsible to follow up until it is approved from parliament.
2.	Draft e-Transaction and e- Signature Law	MCIT, ISSD, MoJ, Parliament	US-DOC, CLDP, Council of Europe, UNCITRAL	June 2017	Draft E-transaction and E-Signature law is ready and it need follow up with MoJ and other relevant government authorities.
3.	Draft National Cyber/Information security Policy	MCIT, ISSD, National Security Council	MCIT	December 2016	Kickoff meeting started in March 2014, Information security policies will be applied once we have ICT infrastructure in place .
4.	Draft ICT Law	MCIT, ISSD, MoJ, Parliament	US-DOC, CLDP, UNCITRAL, IMPACT, Council of Europe	December 2017	Draft ICT law was divided into sections to make it easier for implementation.
5.	Draft Intergovernmental IT security, Router, Switch, Firewall Policies.	MCIT, ISSD	MCIT	December 2014	Kickoff meeting started in August 2014, deadline for implementation of these policies are June 2017.
6.	Draft Computer crime incident response procedure	MCIT, ISSD	MCIT	December 2016	Ready to use by Information System and Security Directorate (ISSD).
7.	IT security training curriculum/schedule & trainings.	MCIT, ISSD, EGRC-II	MCIT, EGRC-II, E-Gov	December 2017	By December 2017 EGRC-II will train 480 employees of government and independent organizations in cyber security training. So far EGRC-II has trained more then 100 employees in cyber security including 38 % females.
8.	Auditing Financial institutes & Government Ministries.	MCIT, ISSD,	MCIT and Attorney General's Office, E-Gov, EGRC-II.	Dec 2017	After implementation of E-Gif standards, EGRC-II will perform auditing and compliance standards of key 13 Ministries.
9.	Guidelines for forensic investigation & Establishment of Forensic Lab	MCIT, ISSD	MCIT, EGRC-II	June 2016	Establishment & testing of Forensic lab will be done till June 2016.
10.	Child Online Protection Policy	MCIT, MoE, NGOs	MCIT and IMPACT	August 2017	Kickoff meeting starts in December 2014.

11.	Ministry of Communication and IT proposed network design	MCIT, E-Gov, ANDC ,EGRC-II	MCIT,	June 2017.	Proposed ICT Network model is ready .
13.	Implementation plan for Public key (PKI)	MCIT, ISSD, ANDC , EGRC-II	MCIT, EGRC-II	December 2017	PKI infrastructure is already in place , EGRC-II will provide funding for trainings , maintenance and roll out of PKI.
14.	Implementing data at rest encryption to protect data	MCIT, ISSD , EGRC-II	MCIT, ISSD, EGRC-II	December 2017	Policies are already defined , requires funding to purchase software's for encryptions.

[1]: Reference: National Cyber Security Strategy Of Afghanistan.

List of all Appendix

13. APPENDIX A1

AfCERT Incident Reporting Form

CONTACT INFORMATION

Name:	Incident number:
Title:	Date:
Agency:	Incident Date (mm/dd/yy): Time (hh:mm:ss am/pm/time zone):
Contact Number:	
Fax:	Email:

INCIDENT SUMMARY

Type of incident detected (check all that apply):

- ☐ Malicious code (Virus, Worm, Trojan)
- ☐ Denial of Service
- ☐ Unauthorized access
- ☐ Rogue access points (wireless)
- ☐ Loss of equipment
- ☐ Web defacement
- ☐ Unauthorized probe/information gathering
- ☐ System misuse
- ☐ Technical vulnerability
- ☐ Others (please specify):

Source information:

IP:	
Name and address:	
Internet service provider:	

Target information:

Owner (System admin/user):	
IP:	
Level of information compromise:	

Location:	

Operating system (including version):	

Number of Hosts Affected:

☐ < 10 ☐ 10 to 50 ☐ 50 to 100 ☐ > 100

Incident level:

☐ Low

☐ Medium

☐ High

Data classification:

☐ Public

☐ Restricted

☐ Confidential

☐ Secret

☐ Top secret

INCIDENT ASSESSMENT

Was system compromised?	
Is active attack currently on going?	
Suspicion of rootkit or keylogger compromise?	
Has compromised system used as a staging point (island hopping) for deeper attacks?	
Length of time system may have been compromised?	
Origin of attacks is from inside or outside?	

ADDITIONAL INFORMATION

Please provide additional information here:

_____

_____

_____

_____

_____

INFORMATION DISCLOSURE

Who can this information be shared with:

☐ Other Agencies ☐ Law Enforcement ☐ IMPACT ☐ **No sharing is Authorized**

SIGNATORY (AfCERT use only)

This report is received by:

Name:

Position:

Date (mm/dd/yy):

Time (hh:mm:ss am/pm):

14. APPENDIX A2

AfCERT Advisory Template

VULNERABILITY

DETAILS	
CVE/CAN Name	
Description	
First Sample Seen	
Discovery Date	
IMPACT Threat Level	
AfCERT Threat Level	
Affected System/Software	
Currently Known Exploits	
Solution	
References	
Credits	
Revisions	

15. APPENDIX A3

AfCERT Advisory Sample

VULNERABILITY
APSB09-15 Security Advisory for Adobe Reader and Acrobat

DETAILS	
CVE/CAN Name	CVE-2007-0048, CVE-2007-0045, CVE-2009-2564, CVE-2009-2979, CVE-2009-2980, CVE-2009-2981, CVE-2009-2982, CVE-2009-2983, CVE-2009-2984, CVE-2009-2985, CVE-2009-2986, CVE-2009-2987, CVE-2009-2988, CVE-2009-2989, CVE-2009-2990, CVE-2009-2991, CVE-2009-2992, CVE-2009-2993, CVE-2009-2994, CVE-2009-2995, CVE-2009-2996, CVE-2009-2997, CVE-2009-2998, CVE-2009-3431, CVE-2009-3458, CVE-2009-3459, CVE-2009-3460, CVE-2009-3461, CVE-2009-3462
Description	A critical vulnerability (CVE-2009-3459) has been identified in Adobe Acrobat and Adobe Reader 9.1.3 and earlier versions on Windows, Unix and OS X. This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Adobe Acrobat and Adobe Reader. User interaction is required in that a user must visit a malicious web site or open a malicious PDF file.
First Sample Seen	10 October 2009
Discovery Date	08 October 2009
IMPACT Threat Level	High
AfCERT Threat Level	High
Affected System/Software	Adobe Reader 9.1.3 for Windows, Macintosh and UNIX Acrobat 9.1.3 for Windows, Macintosh and UNIX Adobe Reader 8.1.6 for Windows, Macintosh and UNIX Acrobat 8.1.6 for Windows, Macintosh and UNIX Adobe Reader 7.1.3 for Windows and Macintosh Acrobat 7.1.3 for Windows and Macintosh

Currently Known Exploits	Troj/PDFJs-DS - CVE-2009-3459
Solution	The official security patch for this vulnerability has not been released by the vendor as of the writing of this advisory. Adobe plans to releases updates for this issue on October 13, 2009. It will be available for download at this URL : http://get.adobe.com/reader/ As a workaround, it is advisable for users to disable the JavaScript feature in Adobe Acrobat and Adobe Reader.
References	http://www.adobe.com/support/security/bulletins/apsb09-15.html
Credits	Adobe
Revisions	14 October 2009 - Initial analysis written

DEFINITIONS

Vulnerability:
Identifier of the vulnerability.

Description:
Summary of the cause and potential effect of the vulnerability provided by IMPACT.

First Sample Seen:
Date of the first sample seen by AfCERT.

Discovery Date:
Date of the earliest known publically disclosed advisory.

IMPACT Threat Level:
Threat level assigned by IMPACT

AfCERT Threat Level:
Threat level assigned by AfCERT

LOW - There is little chance of this vulnerability being actively exploited by malware.
MEDIUM - There is a possibility of this vulnerability being actively exploited by malware.
HIGH - There is a strong possibility of this vulnerability being actively exploited by malware.

Affected System/Software:
Vulnerable platforms and software versions.

Currently Known Exploits:
List of identities for known exploits, if applicable.

Solution:
IMPACT-supplied patch identifier and recommended solution, or workaround if applicable.

DEFINITIONS

Vulnerability:
Identifier of the vulnerability.

Description:
Summary of the cause and potential effect of the vulnerability provided by IMPACT.

First Sample Seen:
Date of the first sample seen by AfCERT.

Discovery Date:
Date of the earliest known publically disclosed advisory.

IMPACT Threat Level:
Threat level assigned by IMPACT

AfCERT Threat Level:
Threat level assigned by AfCERT

LOW - There is little chance of this vulnerability being actively exploited by malware.
MEDIUM - There is a possibility of this vulnerability being actively exploited by malware.
HIGH - There is a strong possibility of this vulnerability being actively exploited by malware.

Affected System/Software:
Vulnerable platforms and software versions.

Currently Known Exploits:
List of identities for known exploits, if applicable.

Solution:
IMPACT-supplied patch identifier and recommended solution, or workaround if applicable.

16. Appendix B1

Firewall Policy

A firewall is an appliance (a combination of hardware and software) or an application (software) designed to control the flow of Internet Protocol (IP) traffic to or from a network or electronic equipment. Firewalls are used to examine network traffic and enforce policies based on instructions contained within the Firewall's Rule set. Firewalls represent one component of a strategy to combat malicious activities and assaults on computing resources and network-accessible information. Other components include, but are not limited to, antivirus software, intrusion detection software, patch management, strong passwords/passphrases, and spyware detection utilities.

Firewalls are typically categorized as either “Network” or “Host”: a Network Firewall is most often an appliance attached to a network for the purpose of controlling access to single or multiple hosts, or subnets; a Host Firewall is most often an application that addresses an individual host (e.g., personal computer) separately. Both types of firewalls (Network and Host) can be and often are used jointly.

This policy statement is designed to:

- Provide guidance on when firewalls are required or recommended. A Network Firewall is required in all instances where Sensitive Data is stored or processed; a Host Firewall is required in all instances where Sensitive Data is stored or processed and the operating environment supports the implementation. Both the Network and Host Firewalls afford protection to the same operating environment, and the redundancy of controls (two separate and distinct firewalls) provides additional security in the event of a compromise or failure.
- Raise awareness on the importance of a properly configured (installed and maintained) firewall.

Audience

This policy is applicable to any and all Directorates, departments, and business units that use Electronic Equipment connected to the MCIT network.

Definition

Term	Definition
Electronic Equipment:	All MCIT-owned or issued and any personally-owned computer or related equipment (e.g., servers, workstations, laptops, PDAs, printers, fax and other such devices) that attaches to the MCIT network, or is used to capture, process or store MCIT data, or is used in the conduct of MCIT business.
Enterprise System:	Applicable to any infrastructure as a means of describing its importance to the MCIT's mission and how it should be administered, protected and funded. From a functional viewpoint, an Enterprise System will be either (a) the only delivery platform for an essential service, or (b) a platform for a service to a very broad constituency spanning organizational boundaries. An Enterprise System is most frequently administered and protected by an institutional unit with expertise in both the technology and the business functions delivered.
Firewall:	Any hardware and/or software designed to examine network traffic using policy statements (ruleset) to block unauthorized access while permitting authorized communications to or from a network or electronic equipment.
Firewall Administrator:	The MCIT function charged with the responsibility of Firewall Configuration and/or Ruleset administration. Administrative duties typically include implementation and documentation of approved changes, analysis of activity logs, and execution and documentation of reviews of system settings and/or rulesets.

Firewall Configuration:	The system settings affecting the operation of a firewall appliance.
Firewall Ruleset:	A set of policy statements or instructions used by a firewall to filter network traffic.
Host:	Any computer connected to a network.
Host Firewall:	A firewall application that addresses a separate and distinct host. Examples include, but are not limited to: Symantec's Norton Personal Firewall, Zone Labs' ZoneAlarm, native firewall functionality supplied under operating systems, e.g., Mac OS X, Linux, Windows 7 (and higher).
Internal Information:	Information that is intended for use by and made available to employees of the MCIT community who have a business need to know. Internal information is not intended for public dissemination but may be released to external parties to the extent there is a legitimate business need. MCIT reserves the right to control the content and format of Internal information when it is published to external parties. Examples include employment data, financial expenditure detail.
Network Device:	Any physical equipment attached to the MCIT network designed to view, cause or facilitate the flow of traffic within a network. Examples include, but are not limited to: routers, switches, hubs, wireless access points.
Network Extension:	Any physical equipment attached to the MCIT network designed to increase the port capacity (number of available ports) at the point of attachment. Examples include, but are not limited to: routers (wired and wireless), switches, hubs, gateways.
Network Firewall:	A firewall appliance attached to a network for the purpose of controlling traffic flows to and from single or multiple hosts or subnet(s).

Public Information:	Information that is available to all members of the MCIT community, and may be released to the general public. The MCIT reserves the right to control the content and format of Public Information. This information is not restricted by local, state, national, or international statute regarding disclosure or use. Examples include the MCIT's auditable financials, schedule of classes, and approved census facts.
Sensitive Data:	Information which is classified for the use of MCIT senior management, staff and partners
MCIT Network:	The network infrastructure and associated devices provided or served by the MCIT.

Policy Statement:

Where Electronic Equipment is used to capture, process or store data identified as MCIT "Legally/Contractually Restricted" and the Electronic Equipment is accessible via a direct or indirect Internet connection, a Network Firewall appropriately installed, configured and maintained is required.

All installations and implementations of and modifications to a Network Firewall and its Configuration and Ruleset are the responsibility of the authorized Firewall Administrator of IT department, Technology and Innovation directorate of MCIT with the support and cooperation of Information Systems Security directorate, with this exception: maintenance of a Network Firewall Ruleset may be performed by other than MCIT personnel where permitted by a documented agreement between MCIT and the third party maintenance contractor assuming the Firewall Administrator's responsibilities.

Where Electronic Equipment is used to capture, process or store data identified as MCIT "Legally/Contractually Restricted" and the Electronic Equipment is accessible via an Internet connection, a Host Firewall appropriately installed, configured and maintained is required where the operating environment supports that installation. The maintenance of the Host Firewall's Configuration and Ruleset is the responsibility of that system's administrator.

Where Electronic Equipment is used to capture, process or store data identified as MCIT "Internal" or "Public" and the Electronic Equipment is accessible via an Internet connection, a Host and/or Network Firewall is recommended.

Use of a Host Firewall is recommended for any individual Host with access to the Internet; its maintenance is the responsibility of the individual user or designated support personnel.

Procedures

1. All Network Firewalls installed and implemented must conform to the current international standards and best security practices. Unauthorized or non-standard equipment is subject to immediate removal, confiscation, and/or termination of network connectivity without notice.
2. A properly executed Risk Acceptance Agreement is required before a directorate, department/Business Unit is permitted to assume the management of a Network Firewall Ruleset. The agreement requires the signature of the individual who will perform Ruleset maintenance (Ruleset administrator) and that of the unit manager, and indicates their acceptance of the risk associated with the activity of Ruleset management.
3. Network Firewall Rulesets

a. The Request for Firewall Ruleset Modification Form is used to:

1. Request and document all changes to Network Firewall Rulesets where Firewall Administration is performed by MCIT. All requests are subject to the approval of Technology and innovation directorate of MCIT and review by ISSD or its designate.
2. Document (only) all changes to Network Firewall Rulesets where Firewall Administration is performed by other than MCIT. Though approval is not required, all requests are subject to review by MCIT.

b. All related documentation is to be retained by the Firewall Administrator for three (3) years and is subject to review by ISSD.

1. All Firewall implementations must adopt the position of "least privilege" and deny all inbound traffic by default (the initial Ruleset should be set to “logging or learning mode” to prevent service interruptions). The Ruleset should be opened incrementally to only allow permissible traffic.
2. Firewalls must be installed within Afghanistan National data Center (ANDC) premises,

3. Firewall Rulesets and Configurations require periodic review to ensure they afford the required levels of protection:

   a. ISSD must review all Network Firewall Rulesets and Configurations during the initial implementation process.

   b. Firewalls protecting Enterprise Systems must be reviewed semi-annually; MCIT Firewall Administrators and ISSD must collaborate on this review.

   c. Firewalls not protecting Enterprise Systems must be reviewed annually by the Responsible firewall administrator.

   d. Firewall Administrators must retain the results of Firewall reviews and supporting documentation for a period of three (3) years; all results and documentation are subject to review by ISSD.
4. Firewall Rule sets and Configurations must be backed up frequently to alternate storage (not on the same device). Multiple generations must be captured and retained in order to preserve the integrity of the data, should restoration be required. Access to Rule sets and configurations and backup media must be restricted to those responsible for administration and review.
5. Any MCIT entity operating under an e-merchant license is required to have properly configured Firewalls in place to protect credit card data and comply with Payment Card Industry/Data Security Standards (PCI/DSS). MCIT will not operate any Firewalls installed for the purpose of PCI/DSS compliance. MCIT requiring PCI/DSS compliance should contract with a PCI-compliant vendor to operate network equipment that falls within PCI/DSS scope and requirements. ISSD will provide technical guidance and coordinate the deployment of required equipment. PCI/DSS Firewalls should include the use of Network Address Translation (NAT) where required to help ensure compliance with PCI/DSS. Any questions about the suitability and use of NAT should be directed to ISSD.
6. Network Firewall administration logs (showing administrative activities) and event logs (showing traffic activity) are to be written to alternate storage (not on the same device) and reviewed at least daily, with logs retained for ninety (90) days. It is recommended that utilities or programs that facilitate the review process be employed. Appropriate

access to logs and copies is permitted to those responsible for Firewall and/or system maintenance, support and review.

7. ISSD Firewall Administrators will execute approved changes to the Firewall Rulesets maintained by IT department of MCIT during the Scheduled Maintenance Window
8. Firewall Administrators of IT department of MCIT will perform changes to Firewall Configurations according to approved production maintenance schedules.

Forms and Instructions:

ISSD will coordinate requests for exceptions to this policy and contact the respective policy owner, data steward and other authorities as deemed appropriate for consideration and discussion of the exception request.

Individuals who discover or strongly suspect a violation of this policy or standards must promptly notify their management and/or any of the following:

AFCERT department of ISSD at MCIT

Directorate of Technology and Innovation of MCIT

Head of Afghanistan National Data Center (ANDC)

17. Appendix B2

1.0. INFORMATION TECHNOLOGY SECURITY POLICY

1.1 Policy statement

"It shall be the sole responsibility of the Information Systems Security Directorate (ISSD) and Technology and Innovation directorate of MCIT to provide adequate protection and confidentiality of all corporate data and proprietary software systems, whether held centrally, on local storage media, or remotely, to ensure the continued availability of data and programs to all authorized staff, and to ensure the integrity of all data and configuration controls."

1.2 SUMMARY OF MAIN SECURITY POLICIES.

1. Confidentiality of all data is to be maintained through discretionary and mandatory access controls, and wherever possible these access controls should meet with international standards or best practices.
2. Internet and other external service access are restricted to authorized personnel only.
3. Access to data on all laptop computers is to be secured through encryption or other means, to provide confidentiality of data in the event of loss or theft of equipment.
4. Only authorized and licensed software may be installed, and installation may only be performed by IT department staff of Technology and Innovation Directorate.
5. The use of unauthorized software is prohibited. In the event of unauthorized software being discovered it will be removed from the workstation immediately.
6. Data may only be transferred for the purposes determined in the MCIT's data-protection policy.
7. All magnetic drives and removable media from external sources must be virus checked before they are used within the MCIT.
8. Passwords must consist of a mixture of at least 8 alphanumeric characters, and must be changed every 40 days and must be unique.
9. Workstation configurations may only be changed by IT department staff.
10. The physical security of computer equipment will conform to recognized loss prevention guidelines.

11. To prevent the loss of availability of IT resources measures must be taken to backup data, applications and the configurations of all workstations.
12. A business continuity plan will be developed and tested on regular bases.

1.3 VIRUS PROTECTION

1. The IT department of Technology and Innovation Directorate will have available up to date virus scanning software for the scanning and removal of suspected viruses.
2. All MCIT severs and corporate file-servers will be protected with virus scanning software.
3. Workstations will be protected by virus scanning software.
4. All workstation and server anti-virus software will be regularly updated with the latest anti-virus patches by the IT department of Technology and Innovation Directorate.
5. No magnetic disk that is brought in from outside the MCIT is to be used until it has been scanned.
6. All systems will be built from original, clean master copies whose write-protection has always been in place. Only original master copies will be used until virus scanning has taken place.
7. All removable media containing executable software (software with .EXE and .COM extensions) will be write- protected wherever possible.
8. All demonstrations by vendors will be run on their machines not the MCIT's.
9. Shareware is not to be used, as shareware is one of the most common infection sources. If it is absolutely necessary to use shareware it must be thoroughly scanned before use.
10. New commercial software will be scanned before it is installed as it occasionally contains viruses.
11. All removable media brought in to the MCIT by field engineers or support personnel will be scanned by the IT Department before they are used on site.
12. To enable data to be recovered in the event of virus outbreak regular backups will be taken by the IT department.

13. Management strongly endorse the MCIT's anti-virus policies and will make the necessary resources available to implement them.

14. Users will be kept informed of current procedures and policies.

15. Users will be notified of virus incidents through AFCERT department of ISSD.

16. Employees will be accountable for any breaches of the MCIT's anti-virus policies.

17. Anti-virus policies and procedures will be reviewed regularly.

18. In the event of a possible virus infection the user must inform the AFCERT department immediately. AFCERT will then scan the infected machine and any removable media or other workstations to which the virus may have spread and eradicate it.

1.4 Access control

1. Users will only be given sufficient rights to all systems to enable them to perform their job function. User rights will be kept to a minimum at all times.
2. Users requiring access to systems must make a written application on the forms provided by the Technology and Innovation Directorate.
3. Where possible no one person will have full rights to any system. The IT department will control network/server passwords and system passwords will be assigned by the system administrator in the end- user department. The system administrator will be responsible for the maintaining the data integrity of the end-user department's data and for determining end-user access rights.
4. Access to the network/servers and systems will be by individual username and password or by smartcard PIN number, biometric.
5. Usernames and passwords must not be shared by users.
6. Usernames and passwords should not be written down.
7. Usernames will consist of initials and surname.
8. All users will have an alphanumeric password of at least 8 characters.

9. Passwords will expire every 40 days and must be unique.
10. Intruder detection will be implemented where possible. The user account will be locked after 3 incorrect attempts.
11. The IT department will be notified of all employees leaving the MCIT's employment. The IT department will then remove the employees' rights to all systems.
12. Network/server supervisor passwords and system supervisor passwords will be stored in a secure location in case of an emergency or disaster, for example a fire safe in the IT department.
13. Auditing will be implemented on all systems to record login attempts/failures, successful logins and changes made to all systems by the ISSD authorized personnel.
14. IT department staff will not login as root on to UNIX, Linux systems, but will use the su command to obtain root privileges.
15. Use of the Administrator username on Windows servers is to be kept to a minimum.
16. Default passwords on systems such as Oracle and SQL Server will be changed after installation.
17. On UNIX and Linux systems, rights to rlogin, ftp, telnet, ssh will be restricted to IT department staff only.
18. Where possible users will not be given access to the UNIX, or Linux shell prompt.
19. Access to the network/servers will be restricted to normal working hours. Users requiring access outside normal working hours must request such access in writing on the forms provided by the Technology and Innovation Directorate
20. File systems will have the maximum security implemented that is possible. Where possible users will only be given Read and Filescan rights to directories, files will be flagged as read only to prevent accidental deletion.

1.5 LAN Security

1.5.1 Hubs & Switches

1. LAN equipment, hubs, bridges, repeaters, routers, switches will be kept in secure hub rooms. Hub rooms will be kept locked at all times. Access to hub rooms will be restricted to IT department and ISSD security staff only. Other staff and contractors requiring access to hub rooms will notify the security staff of ISSD and IT department in advance so that the necessary supervision can be arranged.

1.6 Workstations

2. Users must logout of their workstations when they leave their workstation for any length of time. Alternatively Windows may be locked.
3. All unused workstations must be switched off outside working hours.

1.7 Wiring

4. All network wiring will be fully documented.
5. All unused network points will be de-activated when not in use.
6. All network cables will be periodically scanned and readings recorded for future reference.
7. Users must not place or store any item on top of network cabling.
8. Redundant cabling schemes will be used where possible.

1.8 Monitoring Software

9. The use of LAN analyzer and packet sniffing software is restricted to the AFCERT department of ISSD.
10. LAN analyzers and packet sniffers will be securely locked up when not in use.
11. Intrusion detection systems will implemented to detect unauthorized access to the network

1.9 Servers

12. All servers will be kept securely under lock and key inside racks.

13. Access to the system console and server disk/tape drives will be restricted to authorized IT department and ISSD security staff only.

2.0 Electrical Security

14. All servers will be fitted with UPS's that also condition the power supply.
15. All hubs, bridges, repeaters, routers, switches and other critical network equipment will also be fitted with UPS's.
16. In the event of a mains power failure, the UPS's will have sufficient power to keep the network and servers running until the generator takes over.
17. Software will be installed on all servers to implement an orderly shutdown in the event of a total power failure.
18. All UPS's will be tested periodically.

2.1 Inventory Management

19. The IT department will keep a full inventory of all computer equipment and software in use throughout the Company.
20. Computer hardware and software audits will be carried out periodically via the use of a desktop inventory package. These audits will be used to track unauthorized copies of software and unauthorized changes to hardware and software configurations, only ISSD auditors are authorized to conduct the security audit throughout the MCIT network.

This section applies to Windows, UNIX, Linux and Oracle servers.

2.2 Server Specific Security

1. The operating system will be kept up to date and patched on a regular basis.
2. Servers will be checked daily for viruses.
3. Servers will be locked in a secure room.
4. Where appropriate the server console feature will be activated.
5. Remote management passwords will be different to the Admin/Administrator/root password.
6. Users possessing Admin/Administrator/root rights will be limited to trained members of the IT department staff of Technology and Innovation Directorate only.
7. Use of the Admin/Administrator/root accounts will be kept to a minimum.
8. Assigning security equivalences that give one user the same access rights as another user will be avoided where possible.
9. User's access to data and applications will be limited by the access control features.
10. Intruder detection and lockout will be enabled.
11. The system auditing facilities has to be enabled.
12. Users must logout or lock their workstations when they leave their workstation for any length of time.
13. All unused workstations must be switched off outside working hours.
14. All accounts will be assigned a password of a minimum of 8 characters.
15. Users will change their passwords every 40 days.
16. Unique passwords will be used.
17. The number of grace logins will be limited to 3.
18. The number of concurrent connections will be limited to 1.
19. Network login time restrictions will be enforced preventing users from logging in to the network outside normal working hours.
20. In certain areas users will be restricted to logging in to specified workstations only.

1. Direct root access will be limited to the system console only.
2. IT department staff requiring root access must make use of the su command.
3. Use of the root account will be kept to a minimum.

2.3 UNIX & Linux Specific Security

4. All UNIX and Linux system accounts will be password protected, lp etc.
5. rlogin facilities will be restricted to authorized IT department staff only.
6. ftp facilities will be restricted to authorized I.T. Services staff only.
7. telnet facilities will be restricted to authorized users.
8. ssh facilities will be restricted to authorized users.
9. Users access to data and applications will be limited by the access control features.
10. Users will not have access to the $ prompt.
11. All accounts will be assigned a password of a minimum of 8 characters.
12. Users will change their passwords every 40 days.

1. Wireless LAN's will make use of the most secure encryption and authentication facilities available.

2.4 Wide Area Network Security

2. Users will not install their own wireless equipment under any circumstances.
3. Dial-in modems will not be used if at all possible. If a modem must be used dial-back modems should be used. A secure VPN tunnel is the preferred option.
4. Modems will not be used by users without first notifying the IT department of Technology and Innovation Directorate and obtaining their approval.
5. Where dial-in modems are used, the modem will be unplugged from the telephone network and the access software disabled when not in use.
6. Modems will only be used where necessary, in normal circumstances all communications should pass through the MCIT's router and firewall.
7. Where leased lines are used, the associated channel service units will be locked up to prevent access to their monitoring ports.
8. All bridges, routers and gateways will be kept locked up in secure areas.
9. Unnecessary protocols will be removed from routers.
10. The preferred method of connection to outside MCIT is by a secure VPN connection, using IPSEC or SSL.
11. All connections made to the MCIT's network by outside MCITs will be logged.

2.5 TCP/IP & Internet Security

1. Permanent connections to the Internet will be via the means of a firewall to regulate network traffic.
2. Permanent connections to other external networks, for offsite processing etc., will be via the means of a firewall to regulate network traffic.
3. Where firewalls are used, a dual homed firewall (a device with more than one TCP/IP address) will be the preferred solution.
4. Network equipment will be configured to close inactive sessions.
5. Where modem pools or remote access servers are used, these will be situated on the DMZ or non-secure network side of the firewall.
6. Workstation access to the Internet will be via the MCIT's proxy server and website content scanner
7. All incoming e-mail will be scanned by the MCIT's e-mail content scanner.

2.6 Voice System Security

1. DISA port access (using inbound 0800 numbers) on the PBX will be protected by a secure password.
2. The maintenance port on the PBX will be protected with a secure password.
3. The default DISA and maintenance passwords on the PBX will be changed to user defined passwords.
4. Call accounting will be used to monitor access to the maintenance port, DISA ports and abnormal call patterns.
5. DISA ports will be turned off during non-working hours.
6. Internal and external call forwarding privileges will be separated, to prevent inbound calls being forwarded to an outside line.
7. The operator will Endeavour to ensure that an outside call is not transferred to an outside line.
8. Use will be made of multilevel passwords and access authentication where available on the PBX.
9. Voice mail accounts will use a password with a minimum length of six digits.
10. The voice mail password should never match the last six digits of the phone number.
11. The caller to a voice mail account will be locked out after three attempts at password validation.
12. Dialing calling party pays numbers will be prevented.
13. Telephone bills will be checked carefully to identify any misuse of the telephone system.

18. Appendix B3

3.0 ACCEPTABLE USE POLICY STATEMENT

3.1 System Security Use Policy

You Are Attempting To Logon To And Access Information Systems Owned and Operated By The Ministry Of Communication & Information Technology, Hereafter (Listed As MCIT).

If You Are Not Registered Or Authorized By MCIT Management, Do Not Continue!

It Is the Policy of MCIT That Only Registered and Authorized Employee's And Authorized Users Identified by MCIT Management Gain Access to These Systems. The Use Of These Systems Will Be Specific To The Business MCIT Management Has Directed To Its Employees and Users. The Use Of This System To Intentionally Cause Harm To This System Or Any Of its Connected Peripheral Systems Or Any Other Externally Connected Internet Systems Is Strictly Prohibited And Forbidden. MCIT Reserves The Right To Enforce Accountability And Prosecute Within The Full Limits Of Civil And Criminal Law Currently Available To Those Who Disregard Any Portion Of This Policy.

All MCIT information systems and computers are subject to monitoring at all times to ensure proper functionality of the systems and equipment including security devices in order to prevent unauthorized use and violation of MCIT security policy/regulations.

19. Appendix B4

4.0 ROUTER/SWITCH SECURITY POLICY

4.1 Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of *Ministry of Communications and IT (MCIT)* of Islamic Republic of Afghanistan

4.2 Scope

All employees, contractors, consultants, temporary and other workers at MCIT and its directorates must adhere to this policy. All routers and switches connected to *MCIT* production networks are affected. Routers and switches within internal, secured labs are not affected.

4.3 Policy

Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers must use TACACS+ for all user authentication.
2. The enable secret password on the router must be kept in a secure encrypted form. The router must have the enable secret password set to the current production router password from the Network Operations Center. The enable password command should not be used.
3. Routers must comply with the standards outlined in the Router IOS Template. Routers that do not meet these standards will be re-engineered as needed.
4. The following services or features must be disabled:
    a. *IP directed broadcast*
    b. *Incoming packets at the router sourced with invalid addresses such as RFC1918*
    c. *Incoming packets at the router sourced with MCIT addresses (spoofing)*
    d. *TCP and UDP "small services"*

    e. *All source routing switching*
    f. *All web services running on router*
    g. *Cisco Discovery Protocol (CDP) on internet connected interfaces*
    h. *Telnet, FTP and HTTP services*
    i. *Auto configuration*
5. The following services or features must be disabled unless a business justification is provided:
    a. *CISCO discovery and other discovery protocols*
    b. *Dynamic trunking*
    c. *Scripting environments such as the TCL shell*
6. The following services must be configured:
    a. *Password encryption*
    b. *NTP configured to a corporate standard source*
7. All routing updates shall be done using secure routing updates
8. Use corporate standardized SNMP community strings. Default community strings such as "public" and "private" should never be used. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.
9. Access control list (ACL) must be used to limit the source and type of traffic that can terminate on the device itself.
10. Access control lists for transiting the device are to be added as business needs arise.
11. The router must be included in the corporate enterprise management system with a designated point of contact.
12. Every router should save system logging information to a local RAM buffer in addition to a secured "syslog" server.
13. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSHv2 is preferred management protocol.

14. Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.
15. The corporate router configuration standard will define the category of sensitive routing and switching devices and require additional services or configuration on sensitive device including:
    a. *IP access list accounting*
    b. *Device logging*
    c. *Incoming packets at the router sourced with invalid addresses such as RFC1918 address, or those that could be used to spoof network traffic shall be dropped.*
    d. *Router console and modem access must be restricted by additional security controls*
16. Each router must have the following statement posted in clear view as a banner:

NOTICE: This system is to be used ONLY by AUTHORIZED personnel. Any unauthorized use of the system is unlawful, and may be subject to civil and/or criminal penalties. Use of the system may be logged or monitored without further notice.

17. Security patches and IOS upgrades will be applied as needed during a designated maintenance window. It is the responsibility of the ISSD to keep up-to-date with new security vulnerabilities.

Every switch must meet the following configuration standards:

1. Ports without any need to trunk should have any trunk settings set to off, as opposed to auto.
2. Trunk ports should use a virtual LAN (VLAN) number not used anywhere else in the switch.
3. Disable any port that is not needed.
4. Disable Spanning Tree Port fast on any port that is attached to a router, firewall or load balancing switch.
5. Hard code speed and duplex settings on all ports, as opposed to auto.

6. Core switches must be assigned a private internal IP address in a “management Vlan.”
7. DHCP Snooping should be enabled on all Layer 2 ports.
8. Change default VLAN Name & ID to corporate name and ID..
9. Disable BPDU guard on any port that is not participating in STP election.
10. Disable root guard on any port
11. It is recommended to set all ports without a need to trunk into the DTP off state
12. If VTP is used, be sure to use it with the MD5 digest option.
13. Enable port security by limiting the number of MAC addresses that can communicate on any given port on a switch.

4.4 Policy Compliance

4.4.1 Compliance Measurement

The ISSD team will verify compliance to this policy through various methods, including but not limited to, periodic walk-through, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner (MCIT)

4.4.2 Exceptions

Any exception to the policy must be approved by the ISSD in advance.

4.4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

20. Appendix B5

5.0 SECURITY RECOMMENDATIONS FOR DESKTOP COMPUTERS

Computers are constantly subjected to attempts to exploit system and application vulnerabilities. The ISSD of MCIT offers these recommendations to bolster:

5.1 Background Issues

1. Use Antivirus/Endpoint security software. All computers (PCs and Macs) should have the MCIT provided version of Kaspersky Anti-Virus and should retain the setting that schedules regular updates of virus definitions.
2. When a desktop computer is built, all operating system updates and patches should be applied. In addition, operating system updates and patches should be applied regularly, on an ongoing basis. If possible set the system to do automatic updates. The frequency will be a balance between loss of productivity (while patches are applied) and the need for security.
3. If applicable, use Microsoft Update instead of Windows update to ensure you also update Microsoft Office products.
4. Ensure that other products such as your browser, Java, iTunes, and Adobe Reader and Flash are the latest versions and set to check for updates.
5. Whenever possible, security policies should be set at the server level and applied to the desktop machines.
6. Do not use the administrator account as the regular login account. Create a separate login account for each user of the system.
7. To keep in line with noted passwords use the following rules to create a “strong” password, defined as:

- must be 8-31 characters in length
- must include punctuation such as (!] & * , + =
- must not include the characters ^ $ ' " # < ? @ | ` \
- Passwords should be changed every year at a minimum.

8. The guest account should be disabled.

9. New machines with Windows or OS X should activate the built-in firewall.
10. All machines with Windows XP SP2+ should be checked with the Microsoft Baseline Security analyzer for obvious security holes.
11. All compromised machines should be rebuilt from scratch (i.e. erase the hard drive and start fresh from installation disks).
12. Do not install Microsoft IIS or turn on any of its functions unless absolutely necessary.
13. In general, start from a position of security that is most secure (i.e. no shares, no guest access, etc.) and open up services as necessary.

In addition to the above suggestions, ISSD of MCIT recommends a regular backup strategy. It should be noted that even with all the procedures listed above, there is still the possibility of a virus infection or hacker compromise. Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine.

When a compromised machine is detected, AFCERT security will shut the port off; this will isolate the desktop computer until it can be rebuilt.

NOTE: Do not move or connect a compromised machine to another active port – this will result in that port also being shut off as the compromised machine is detected.

Once the computer has been rebuilt and brought current, and AFCERT security notified, the port will be returned to active status.

For departments with their own subnets and administrators, standard filters can be applied at the subnet level. If a department has its own servers, AFCERT security personnel can scan the servers, Web sites and Web applications for vulnerabilities upon request.