GENERAL INFORMATION SECURITY BEST PRACTICE GUIDE

Preamble

1. Introduction

The Communications Authority of Kenya (CA) is the regulatory Authority for the ICT industry in Kenya with responsibilities in telecommunications, cybersecurity, e-commerce, broadcasting and postal/courier services. CA is also responsible for managing the country's numbering and frequency spectrum resources as well safeguarding interests of consumers of ICT services. CA's mandate is drawn from the Kenya Information and Communications Act, as Amended.

Under Sections 83C of the KICA, CA is mandated to develop a framework for facilitating the investigation and prosecution of cybercrime offenses, and to promote and facilitate the efficient management of critical Internet resources. Pursuant to this, CA established the National Kenya Computer Incident Response Team - Coordination Centre (National KE-CIRT/CC) which is responsible for national coordination and response to cyber threats. The National KE-CIRT/CC is also Kenya's national point of contact on cyber security matters. Further, the Kenya Information and Communications (Consumer Protection) Regulations, 2010, provide for safeguards for the security of ICT services, the protection of children, and unsolicited communication, among other consumer protection issues.

Based upon this mandate, CA in collaboration with various stakeholders including but not limited to the banking sector, telecommunication companies, internet service providers, academia, government agencies including law enforcement, the domain name sector, professional associations and public utility companies, now issues this Guide as information security best practices.

2. The Purpose of the Guide

The aim is the adoption of this Guide by Kenyan organizations and users across all sectors to enable them to deal with common information security challenges.

The Guide provides good information security practices. It does not prescribe any specific practices or standards that must be implemented. It acknowledges the culture and uniqueness of the Kenyan cyber space in relation to information security. This Guide is meant to improve Kenya's cyber security posture especially among Small and Medium Enterprises (SMEs), government, private sector players and the general public. This Guide complements already existing policies, standards and nothing in this document should be taken to contradict standards and guidelines that are mandatory and binding on the users or providers of ICT services.

3. Definitions and Abbreviations

3.1. "Availability" means ensuring that authorized users have access to information and associated assets when required.

3.2. "Bring Your Own Device" (BYOD) means bring your own phone (BYOP), and bring your own Personal Computer (BYOPC) and refers to the policy of permitting employees to bring

personally owned devices (laptops, tablets, and smartphones) to their workplace, and to use those devices to access privileged company information and applications.

3.3. "Computer Hardening" means the process of securing a system by reducing its areas of weakness.

3.4. "Confidentiality" means that the information is not made available for disclosure to unauthorized individuals, entities, or processes.

3.5. "Cyberattack" means any type of offensive maneuver employed by nation-states, individuals, groups, or organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by gaining unauthorized access into a susceptible system.

3.6. "Encryption" means the process of encoding a message or information in such a way that only authorized parties can access it.

3.7. "Integrity" means the maintenance and safeguarding of the accuracy, consistency and completeness of data over its entire life-cycle including processing methods.

3.8. "Log" means an electronic record of events that occur in a computer system (operating systems, software frameworks, programs). These records contain events that occur in the computer system or activities carried out by the users of a computer system.

3.9. "Multi-factor authentication (MFA)" means a method of computer access control in which a user is granted access only after successfully presenting several separate pieces of identity to an authentication mechanism.

3.10. "National KE-CIRT/CC" refers to Kenya's national point of contact on cyber security matters, and is responsible for national coordination and response to cyber threats.

3.11. "NIST" refers to the National Institute of Standards and Technology (NIST).

3.12. "Penetration Testing" means an authorized simulated attack on a computer system that checks for security weaknesses, potentially gaining access to the system's features and data.

3.13. "Personally Identifiable Information (PII)" means any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another can be considered PII – National Identity (ID) number, KRA PIN number, Full Name, etc.

3.14. "Pharming" means a cyber-attack intended to redirect a website's traffic to another fake site that appears like the authentic website.

3.15. "Phishing" means an attempt to obtain sensitive information such as usernames, passwords, PINs and credit card details often for malicious reasons, by pretending to be a trustworthy entity in an electronic communication such as email.

3.16. "Unauthorized access" means the ability to access a computer system without permission. It includes gaining physical access to areas and objects without permission.

4. Proposed Recommendations for Common Information Security Challenges

4.1 Online Safety

Online safety or Internet safety is the knowledge and practice of maximizing the user's personal safety against security risks to private information and property associated with using the Internet.

The major challenges on these issues are security risks to private information associated with using the Internet. The recommended solutions are:

4.1.1 Deployment of protective mechanisms using technology such as antivirus solutions, firewalls, virtual private networks,

4.1.2 Use of good practices such as privacy settings, strong passwords, strong authentication, selective online sharing,

4.1.3 Conduct user awareness on online safety on the said measures.

4.2 Unauthorized Access

Protecting systems, applications and data against unauthorized access is an important element in information security. Unauthorized access may result in breach of confidentiality, alteration or loss of information.

It is recommended that the following solutions be deployed:

4.2.1 Grant limited access on a need-to-have basis,

4.2.2 Use of strong credentials (Password, PIN, Passcode, Biometric),

4.2.3 Use of multi-factor authentication,

4.2.4 Hardening computer systems,

4.2.5 Deployment of security technologies such as firewalls, antivirus, intrusion detection systems among others,

4.2.6 Use of encryption where possible,

4.2.7 Regular software updates,

4.2.8 Maintain and monitor logs,

4.2.9 Conduct system vulnerability assessments, penetration testing and remediate,

4.2.10 Conduct user awareness.

4.3 Governance and Compliance

This is the process of establishing a management framework to initiate and control the implementation and operation of information security.

Users may apply the measures listed below to mitigate risks and challenges related to governance and compliance.

4.3.2 Document and enforce policies, standards, procedures and processes,
4.3.3 Having well defined structures, roles and responsibilities,
4.3.4 Conduct periodic audits,
4.3.5 Conduct Information Security Risk assessment,
4.3.6 Uptake of cybersecurity insurance,
4.3.7 Design and implement business continuity and disaster recovery plans,
4.3.8 Proper management of third parties and vendors,
4.3.9 Understanding the risks that come as a result of outsourcing the specific services as well as putting in place the necessary governance steps to mitigate these risks,
4.3.10 Conducting user awareness.

4.4 Infringement of Intellectual Property (IP) and Trade Secrets

Intellectual Property is valuable to an organization or user and needs to be protected. This includes innovations, such as software applications, that have been developed by an individual or an organization. Infringement of intellectual property and trade secrets can result in loss of revenue and reputation.

To mitigate this, some of the measures to be taken may include:

4.4.1 Registration of copyright, patent, trademark with relevant authorities,
4.4.2 Verification of domain ownership and dispute resolution,
4.4.3 Conducting awareness on intellectual property rights and protection,
4.4.4 Employ information classification policies,
4.4.5 Implement system controls to protect intellectual property.

4.5 Malware

Malware is malicious software that is harmful to computer systems. Examples of malware include; viruses, worms and ransomware.

Malware attacks may be mitigated by:

4.5.1 Deploying security solutions such as antivirus, firewalls, intrusion, detection and prevention systems,
4.5.2 Conducting regular software updates,
4.5.3 Doing regular backups,
4.5.4 System hardening,
4.5.5 Conducting user awareness.

4.6 Social Engineering

Social engineering involves the psychological manipulation of people into divulging confidential information. Social engineering includes phishing, pharming, fraudulent messages or calls among others. To mitigate social engineering, organizations may conduct extensive user awareness to alert users and report such cases to the relevant authorities.

4.7 Cloud Computing

The practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. Cloud computing presents a number of challenges for users and businesses such as:

4.7.1.2 Reliability,
4.7.1.3 Compromised credentials and account hijacking,
4.7.1.4 Jurisdiction,
4.7.1.5 Lack of privacy,
4.7.1.6 Unsecure interfaces,
4.7.1.7 Distributed Denial of Service,
4.7.1.8 Increased risk through shared technology,
4.7.1.9 Cloud service abuses,
4.7.1.10 Limitations in investigations,
4.7.1.11 Governance and Compliance.

To mitigate these, some of the measures to be taken may include:

4.7.2.1 Use of multi-tenancy architecture,
4.7.2.2 Backups / Disaster recovery,
4.7.2.3 Deploy Authentication / Complex passwords,
4.7.2.4 Draw contracts and Service Level Agreements with information security clauses,
4.7.2.5 Patching and update of software and applications,
4.7.2.6 Monitoring and notifications on any security related issues,
4.7.2.7 Use encryption,
4.7.2.8 Local cloud solutions for sensitive information such as private information about citizens and PII,
4.7.2.9 Compliance and auditing.

4.8 Wireless Networks

Wireless networks are widely available and are increasingly becoming free or cheap. However, unsecure wireless networks can allow anyone with a wireless enabled device to connect to a network or other devices in an unsecure manner. Unsecured wireless networks pose various threats to users and organizations.

This Guide proposes that users deploy the following solutions:

4.8.1 Use Secure Connections

Users can add a layer of encryption to the communication by enabling the "Always Use HTTPS" option on websites that the user visits frequently, or that require the user to enter some kind of credentials.

4.8.2 Turn off file-sharing from your device.

4.8.3 Turn wireless off when you don't need it.

4.8.4 Use Internet security solution such as anti-virus.

4.8.5 Download wireless drivers from trusted sources.

4.8.6 Proper Network Configuration: This involves ensuring the setup and configuration of network devices is well done and documented. An example of this is network segmentation.

4.8.7 Use of Virtual Private Network (VPN) where applicable

A virtual private network (VPN) connection is used when connecting to business systems through an unsecured connection. Even if an attacker manages to position themselves in the middle of the connection, the data here will be strongly encrypted.

4.8.8 Use of Public Wireless Networks

Users should refrain from using public wireless networks, such as hotspots, to access sensitive services such as online banking services, among others.

4.8.1 Mobile Security

To secure information stored in a mobile device, the general guide is provided as below:

4.8.1.1. Password-protect your Mobile Device

Choose a strong password. The security of your system is only as strong as the password you select to protect it.

4.8.1.2. Use Anti-malware Applications

Mobile devices can be just as susceptible to malware and viruses as desktop computers.

4.8.1.3. Encrypt Your Mobile Device Where Possible

Use default encryption automatically which comes with the iPhone/iPad 3 and later, and Android phones/tablets.

4.8.1.4. Disable Options and Applications that you Don't Use

Reduce security risk by limiting your device to only necessary applications and services.

4.8.1.5. Regularly Backup your Data

Regularly have a backup copy of any necessary data in case your mobile device is lost or damaged.

4.8.1.6. Follow-up Safe Disposal Practices

When you are ready to dispose off your device, be sure to remove all sensitive information first.

4.8.1.7. Keep Your Operating System Up-to-date

Regularly accept updates and patches to your mobile device's operating software by enabling automatic updates, or accept updates when prompted.

4.8.1.8. Verify Applications before Downloading

Make sure that you download applications from well-known trusted sources.

4.8.2 Systems Unavailability

This is when normal system functions are rendered unusable for reasons not limited to natural disasters, hardware failure, data corruption, data loss, malware, denial of service (DOS). Users are prevented from accessing a critical service.

The recommended solutions are:

a. Frequent backup critical data,
b. Setup a disaster recovery plan,
c. Put in place a Business Continuity planning (BCP): This is a proactive activity done by organizations and individuals to plan/prepare on how to handle system unavailability occurrences. It includes having multiple facilities, equipment, systems, personnel that can be used interchangeably.

4.9 System Fraud

This is deliberate manipulation or modification of data and/or records for financial or personal gain.

The recommended solutions are:

4.9.1 Strong authorization, authentication and identification measures should be implemented across all systems and processes,

4.9.2 Security controls (physical, administrative and technical) should be enforced. This can be achieved through:

4.9.2.1 **Technical or Logical** - Involves hardware or software mechanisms to manage access and to provide protection for resources and systems. Examples include authentication methods (such as usernames, passwords, smartcards, and

biometrics), encryption, constrained interfaces, access control lists, protocols, firewalls, routers and Intrusion Detection Systems (IDSs).

4.9.2.2 **Physical** - They include physical mechanisms (elements that one can touch) deployed to prevent, monitor, or detect direct contact with systems or areas within a facility. Examples include guards, fences, motion detectors, locked doors, sealed windows, lights, cable protection, laptop locks, badges, swipe cards, guard dogs, video cameras, mantraps, and alarms.

4.9.2.3 **Administrative or Management** - These are policies and procedures defined by an organization/person. They focus on personnel and business practices. Examples include policies, procedures, hiring practices, background checks, data classifications and labeling, security awareness and training efforts, leave history, reports and reviews, work supervision, personnel controls, and testing.

4.9.2.4 Auditing and monitoring of systems and processes should be done periodically to detect attempted and successful frauds.

4.9.2.5 Reconciliations should be done by comparing records to ensure accuracy and completeness.

4.9.2.6 Rotation and segregation of duties.

4.9.2.7 User information security awareness/education programs should be put in place to teach and/or remind people about how to recognize and defeat fraud. These should be conducted regularly.

4.10 Identity Theft

This is where someone uses another person's identity information such as a name, identity number, passport number, PIN, social media account, among others without permission.

These can be addressed through:

4.10.11 User education/awareness to teach people to safeguard and secure their personally identifiable information,

4.10.12 Implementing strong authentication procedures/measures in electronic systems,

4.10.13 Reporting of any cases of impersonation immediately to the nearest police station.

4.11 Fake News

The spread of untrue or misleading information over electronic media especially social media is on the increase.

This can be mitigated by:

a) Education and creating awareness about how to recognize fake news, and the dangers of spreading fake news,
b) Users should avoid sharing information that they are not sure about,
c) Reporting to the relevant organizations.

4.12 Information Security Awareness among Users/Organizations

Lack of security awareness by users is a major challenge in safeguarding information security. It is therefore imperative that users are educated on security measures to apply in order to ensure the safety of their information.

To create security awareness among users:

4.12.1 Organizations should create information security awareness for the consumers of its products and/or services,

4.12.2 Awareness material should be delivered in a simple and clear manner that is easily understood by the target audience,

4.12.3 The following topics should *inter alia* be included in the awareness by users:

- 4.12.3.1 Data Privacy,
- 4.12.3.2 Identity Management,
- 4.12.3.3 Outsourced Services,
- 4.12.3.4 Data Backup,
- 4.12.3.5 Intellectual Property,
- 4.12.3.6 Identity Theft,
- 4.12.3.7 Fake News,
- 4.12.3.8 Social Engineering,
- 4.12.3.9 Reporting and responsible disclosure.

4.13 Bring Your Own Device (BYOD)

This is the practice of employees or contractors using their own computers, smartphones, or other devices for work purposes. The practice is increasingly gaining popularity in Kenya.

To address some of the information security challenges posed by this practice, the following measures can be adopted:

4.13.1 These devices should be accorded the same level of security as an organization's information assets,

4.13.2 Devices that hold Personally Identifiable Information (PII) should be encrypted and its loss reported to the relevant agencies,

4.13.3 Organizations should put in place the ability to delete confidential information from such devices, including remotely, in the event of loss/theft,

4.13.4 Contractors/employees under BYOD should have a structured exit plan that protects the organizations information assets,

4.13.5 Establishment of a BYOD Policy.

4.14 Handheld and Mobile Devices

The increased penetration of mobile phones presents various challenges including loss of handheld and mobile devices, loss of Personal Identifiable Information (PII), data loss and exposure of confidential information. Additionally, spread of malicious applications through handheld and mobile devices is on the increase. To address these challenges users should:

4.14.1 Exercise caution in handling mobile and handheld devices,

4.14.2 Minimize storage of critical information on mobile devices,
4.14.3 Download mobile applications from genuine sources,
4.14.4 Delete unnecessary applications from mobile and handheld devices,
4.14.5 Have the ability to delete confidential information from such devices in the event of loss/theft, including remotely.

4.15 Cyber Incident Reporting

The level of cyber incident reporting in the country is very low and vague. In order to increase the quality of information relating to cyber incidents, improve information sharing, situational awareness and faster incident resolution and response, as well as focus on the key risk areas:

4.15.1 User should be educated on what, how and where to report information security incidents,
4.15.2 Organizations should have a point-of-contact for reporting cyber security incidents,
4.15.3 Industry's should establish Sector Computer Incident Response Teams (sCIRT) to enhance coordination and information sharing,
4.15.4 It is recommended that cyber incidents should be reported using a prescribed incident reporting format,
4.15.5 Anonymous reporting should be put in place to encourage responsible disclosure.

Information security efforts are coordinated at the national level by the National KE-CIRT/CC.

5. Recommended Standards

Organizations are encouraged to use international interoperable standards and specifications relevant to network and information security such as ISO/IEC and NIST, among others.

6. Contacting the National KE-CIRT/CC

For advice on cyber security matters, including response to cyber threats, you may reach the National KE-CIRT/CC through either of the following:

Email: incidents@ke-cirt.go.ke
Dedicated 24/7 Hotlines: +254-703-042700/+254-730-172700
National KE-CIRT/CC website: http://www.ke-cirt.go.ke