

ANNEXURE II

GUIDELINES, OPERATIONAL & TECHNICAL STANDARDS



To

THE EKITI STATE ICT POLICY DOCUMENT

AUGUST, 2013

EKSG Guidelines, Operational & Technical Standards (GOTS)

Introduction:

These Guidelines, Operational and Technical Standards establish high-level rules to protect EKSG's technology resources and the data stored by those resources. These GOTS exist at many different levels in this government and her MDAs.

The EKSG ICT GOTS are contained in many documents. This document highlights the various GOTS documents that together support the main ICT Policies and are consequently annexed to it. This document is a living document and continues to be improved upon through version updates.

Our current GOTS comprises of the followings:

Acceptable Use and ethical standard	Appendix 1
Email Standard	Appendix 2
Network and Infrastructure security standard (NISS)	Appendix 3
Third-party connectivity standard	Appendix 4

Each of the above indicated standards documents are now annexed to this introductory page.

Appendix 1

Acceptable Use and Ethical Standards

Ethical Standards

1,0 Overview

EKSG's purpose for this ethics standards is to establish a culture of openness, trust and integrity in business practices. Effective ethics is a team effort involving the participation and support of every EKSG's employee. All employees should familiarize themselves with the ethics guidelines that follow this introduction.

EKSG is committed to protecting employees, partners, vendors and the Government from illegal or damaging actions by individuals, either knowingly or unknowingly. When EKSG addresses issues proactively and uses correct judgment, it will help set us apart from competitors.

EKSG will not tolerate any wrongdoing or impropriety at anytime. EKSG will take the appropriate measures and act quickly in correcting the issue if the ethical code is broken. Any infractions of this code of ethics will not be tolerated.

1. Purpose

Our purpose for authoring a publication on ethics is to emphasize the employee's and consumer's expectation to be treated to fair business practices. These standards will serve to guide business behavior to ensure ethical conduct.

2. Scope

These standards apply to employees, contractors, consultants, temporaries, and other workers at EKSG including all personnel affiliated with third parties.

3. Standards

3.1. Executive Commitment to Ethics

- 3.1.1. Top brass and Senior Government Officials within EKSG must set a prime example. In any business practice, honesty and integrity must be top priority for executives.
- 3.1.2. Executives must have an open door standards and welcome suggestions and concerns from employees. This will allow employees to feel comfortable discussing any issues and will alert executives to concerns within the work force.
- 3.1.3. Executives must disclose any conflict of interests regard their position within EKSG.

3.2. Employee Commitment to Ethics

- 3.2.1. EKSG's employees will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices.
- 3.2.2. Every employee needs to apply effort and intelligence in maintaining ethical value.
- 3.2.3. Employees must disclose any conflict of interests regarding their position within EKSG.
- 3.2.4. Employees will help EKSG to increase customer and vendor satisfaction by providing quality products and timely response to inquiries.

3.3. Government Awareness

- 3.3.1. Promotion of ethical conduct within interpersonal communications of employees will be rewarded.
- 3.3.2. EKSG will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the Government.

3.4. Maintaining Ethical Practices

- 3.4.1. EKSG will reinforce the importance of the integrity message and the tone will start at the top. Every civil servant and political appointees - employee, manager, director needs consistently maintain an ethical stance and support ethical behavior.
- 3.4.2. Employees at EKSG should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.

3.4.3. EKSG has established a best practice disclosure committee to make sure the ethical code is delivered to all employees and that concerns regarding the code can be addressed.

3.5. Unethical Behavior

3.5.1. EKSG will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications.

3.5.2. EKSG will not tolerate harassment or discrimination.

3.5.3. Unauthorized use of Government trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our Government will not be tolerated.

3.5.4. EKSG will not permit impropriety at any time and we will act ethically and responsibly in accordance with laws.

3.5.5. EKSG employees will not use corporate assets or business relationships for personal use or gain.

4. Enforcement

4.1. Any infractions of this code of ethics will not be tolerated and EKSG will act quickly in correcting the issue if the ethical code is broken.

4.2. Any employee found to have violated this standards may be subject to disciplinary action, up to and including termination of employment

6.0 Acceptable Use Standards

6.1` Overview

EKSG's intentions for publishing an Acceptable Use Standards are not to impose restrictions that are contrary to EKSG's established culture of openness, trust and integrity. EKSG is committed to protecting her employees, partners and itself from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the properties of EKSG. These systems are to be used for business

purposes in serving the interests of the Government, and of our clients and customers in the course of normal operations. [Please review the Department of Establishment/Human Resources policies and Civil Service Code of Conduct for further details.](#)

Effective security is a team effort involving the participation and support of every EKSG employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this standards is to outline the acceptable use of computer equipment at EKSG. These rules are in place to protect the employee and EKSG. Inappropriate use exposes EKSG to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This standards applies to employees, contractors, consultants, temporaries, and other workers at EKSG, including all personnel affiliated with third parties. This standards applies to all equipment that is owned or leased by EKSG.

4.0 Standards

4.1 General Use and Ownership

1. While EKSG's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of EKSG. Because of the need to protect EKSG's network, management cannot guarantee the confidentiality of information stored on any network device belonging to the Government.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental and/or unit policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. The Government recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see EKSG's

Information Sensitivity Standards. For guidelines on encrypting email and documents, [go to EKSG's Awareness Initiative](#).

4. For security and network maintenance purposes, authorized individuals within the Government may monitor equipment, systems and network traffic at any time, per Government's Audit Standards.
5. EKSG reserves the right to audit networks and systems on a periodic basis to ensure compliance with these standards.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: Government state data, trade secrets, specifications, citizens information, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. [System level passwords should be changed quarterly; user level passwords should be changed every six months](#).
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at [10 minutes or less](#), or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.
4. Use encryption of information in compliance with EKSG's Acceptable Encryption Use standards.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the [“Laptop Security Tips”](#).
6. Postings by employees from a EKSG’s email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of EKSG unless posting is in the course of business duties.
7. All hosts used by the employee that are connected to the EKSG Internet/Intranet/Extranet, whether owned by the employee or EKSG shall be continually

executing approved virus-scanning software with a current virus database unless overridden by departmental or group standards.

8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of EKSG authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing EKSG owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or Government protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by EKSG.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which EKSG or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a EKSG computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in Nigeria.
7. Making fraudulent offers of products, items, or services originating from any EKSG account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to EKSG is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, EKSG employees to parties outside EKSG.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within EKSG's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by EKSG or connected via EKSG's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.4. Blogging

1. Blogging by employees, whether using EKSG's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Standards. Limited and occasional use of EKSG's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate EKSG's standards, is not detrimental to EKSG's best interests, and does not interfere with an employee's regular work duties. Blogging from EKSG's systems is also subject to monitoring.
2. EKSG's Confidential Information standard also applies to blogging. As such, Employees are prohibited from revealing any EKSG confidential or proprietary information, trade secrets or any other material covered by EKSG's Confidential Information standards when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of EKSG and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by EKSG's Non-Discrimination and Anti-Harassment standards.
4. Employees may also not attribute personal statements, opinions or beliefs to EKSG when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in

blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of EKSG. Employees assume any and all risk associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, EKSG's trademarks, logos and any other EKSG's intellectual property may also not be used in connection with any blogging activity

5.0 Enforcement

Any employee found to have violated these standards may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Term	Definition
-------------	-------------------

<i>Blogging</i>	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.
-----------------	--

<i>Spam</i>	Unauthorized and/or unsolicited electronic mass mailings.
-------------	---

Appendix 2

Email Standards

1.0 Purpose

To prevent tarnishing the public image of EKSG when email goes out from the Government the general public will tend to view that message as an official standards statement from the EKSG.

2.0 Scope

This standards covers appropriate use of any email sent from EKSG's email address and applies to all employees, vendors, and agents operating on behalf of the Government

3.0 Standards

3.1 Prohibited Use. The EKSG's email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Government employee should report the matter to their supervisor immediately.

3.2 Personal Use.

Using a reasonable amount of EKSG's resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from EKSG's email account is prohibited. Virus or other malware warnings and mass mailings from EKSG shall be approved by Government's General Manager, Head of Operations or Head of Information Technology before sending. These restrictions also apply to the forwarding of mail received by EKSG's employee.

3.3 Monitoring

EKSG's employees shall have no expectation of privacy in anything they store, send or receive on the Government's email system. EKSG may monitor messages without prior notice. EKSG is not obliged to monitor email messages.

4.0 Enforcement

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

6.2 Definitions

Term	Definition
Email	The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Eudora and Microsoft Outlook.
Forwarded email	Email resent from an internal network to an outside point.
Chain email or letter	Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.
Sensitive information	Information is considered sensitive if it can be damaging to the Government or its customers' reputation or market standing.
Virus warning.	Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people, both inside and outside EKSG who do not have a need to know that information.
Government	Government wherever used in this document or any other document(s) that are related to this IT Policies means EKSG.

6.4 Revision History

Email Retention Standards

1.0 Purpose

The Email Retention Standards is intended to help employees determine what information sent or received by email should be retained and for how long.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via electronic mail or instant messaging technologies.

All employees should familiarize themselves with the email retention topic areas that follow this introduction.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to Information Technology Unit.

2.0 Scope

This email retention standard is secondary to EKSG's standards on [Freedom of Information and Government Record Keeping](#). Any email that contains information in the scope of the Business Record Keeping standards should be treated in that manner. All Government's email information is categorized into four main classifications with retention guidelines:

Administrative Correspondence **(10 years)**

Fiscal and Financial Correspondence **(10 years)**

General Correspondence **(10 years)**

Ephemeral Correspondence **(Retain until read, destroy)**

3.0 Standards

3.1 Administrative Correspondence

EKSG's Administrative Correspondence includes, though is not limited to clarification of established Government standards, including holidays, time card information, dress code, work place behavior and any legal issues such as intellectual property violations. All email with the information sensitivity label Management Only shall be treated as Administrative Correspondence. To ensure Administrative Correspondence is retained, a mailbox admin@ekitistate.gov.ng has (to be) been created, if you copy (cc) this address when you send email, retention will be administered by the DICT.

3.2 Fiscal and Financial Correspondence

EKSG's Fiscal Correspondence is all information related to revenue and expense for the Government. To ensure Fiscal Correspondence is retained, a mailbox fiscal@ekitistate.gov.ng has (to be) been created, if you copy (cc) this address when you send email, retention will be administered by the DICT.

3.3 General Correspondence

EKSG's General Correspondence covers information that relates to customer interaction and the operational decisions of the business. The individual employee is responsible for email retention of General Correspondence.

3.4 Ephemeral Correspondence

EKSG's Ephemeral Correspondence is by far the largest category and includes personal email, requests for recommendations or review, email related to product development, updates and status reports.

3.5 Instant Messenger Correspondence

EKSG's Instant Messenger General Correspondence may be saved with logging function of Instant Messenger, or copied into a file and saved. Instant Messenger conversations that are

Administrative or Fiscal in nature should be copied into an email message and sent to the appropriate email retention address.

3.6 Encrypted Communications

EKSG's encrypted communications should be stored in a manner consistent with EKSG's Information Sensitivity Standards, but in general, information should be stored in a decrypted format.

3.7 Recovering Deleted Email via Backup Media

EKSG maintains backup tapes from the email server and once a quarter a set of tapes is taken out of the rotation and they are moved offsite. No effort will be made to remove email from the offsite backup tapes.

4.0 Enforcement

Any employee found to have violated these standards may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms and Definitions

Approved Electronic Mail

Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [\[Microsoft Exchange Server, xxxxxx\]](#).

Approved Encrypted email and files

Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within EKSG is done via a license.

Approved Instant Messenger

Skype, Yahoo Messenger IM Clients are the only IM that is approved for use on EKSG computers.

Individual Access Controls

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the `chmod` command (use *man chmod* to find out more about it). On Mac's and PC's, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of EKSG.

Encryption

Secure EKSG Sensitive information in accordance with the *Acceptable Encryption Standards*. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

Network and Infrastructure security standards (NISS)

1.0 Information Sensitivity Standards

1.1.0 Purpose

The Information Sensitivity Standards is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of EKSG without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect EKSG confidential information (e.g., EKSG Confidential information should not be left unattended in conference rooms).

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to IT or Security and Risk or Compliance units.

1.2.0 Scope

All EKSG information is categorized into two main classifications:

- EKSG Public
- EKSG Confidential

EKSG Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to EKSG Card Management Limited.

EKSG Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our Government. Also included in EKSG Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of EKSG Confidential information is "EKSG Third Party Confidential" information. This is confidential information belonging or pertaining to another Government or organization which has been entrusted to EKSG by that Government or organization under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into EKSG's network to support our operations.

EKSG personnel are encouraged to use common sense judgment in securing EKSG Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager

1.3.0 Standards

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as EKSG Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the EKSG Confidential information in question.

1.3.1 Minimal Sensitivity: General corporate information; some personnel and technical information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "EKSG Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "EKSG Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, EKSG information is presumed to be "EKSG Confidential" unless expressly determined to be EKSG Public information by a EKSG employee with authority to do so.

Access: EKSG employees, contractors, people with a business need to know.

Distribution within EKSG: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of EKSG internal mail: NIPOST and other public or private carriers, approved electronic mail and electronic file transmission methods.

Electronic distribution: No restrictions except that it be sent to only approved recipients.

Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on EKSG premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

1.3.2 More Sensitive: Business, financial, technical, and most personnel information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "EKSG Confidential" or "EKSG Proprietary", wish to label the information "EKSG Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

Access: EKSG employees and non-employees with signed non-disclosure agreements who have a business need to know.

Distribution within EKSG: Standard inter-office mail, approved electronic mail and electronic file transmission methods.

Distribution outside of EKSG internal mail: Sent via NIPOST or approved private carriers.

Electronic distribution: No restrictions to approved recipients within EKSG, but should be encrypted or sent via a private link to approved recipients outside of EKSG premises.

Storage: Individual access controls are highly recommended for electronic information.

Disposal/Destruction: In specially marked disposal bins on EKSG premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

1.3.3 Most Sensitive: Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our Government

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that EKSG Confidential information is very sensitive, you may or should label the information "EKSG Internal: Registered and Restricted", "EKSG Eyes Only", "EKSG Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of EKSG Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Access: Only those individuals (EKSG employees and non-employees) designated with approved access and signed non-disclosure agreements.

Distribution within EKSG: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.

Distribution outside of EKSG internal mail: Delivered direct; signature required; approved private carriers.

Electronic distribution: No restrictions to approved recipients within EKSG, but it is highly recommended that all information be strongly encrypted.

Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.

Disposal/Destruction: Strongly Encouraged: In specially marked disposal bins on EKSG premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

1.4.0 Enforcement

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

1.5.0 .Definitions

Terms and Definitions

NIPOST Nigerian Post Office, Nigerian Postal Agency

Appropriate measures

To minimize risk to EKSG from an outside business connection EKSG computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access EKSG corporate information, the amount of information at risk is minimized.

Configuration of EKSG-to-other business connections

Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required

Do not leave in interoffice mail slot, call the mail room for special pick-up of mail.

Approved Electronic File Transmission Methods

Includes supported FTP clients and Web browsers.

Envelopes Stamped Confidential

You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

Approved Electronic Mail

Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, Microsoft Outlook agent and Microsoft Exchange Service.

Approved Encrypted email and files

Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within EKSG is done via a license. Please contact the IT unit if you require a license.

Government Information System Resources

Government Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

Expunge

To reliably erase or expunge data on a PC you must use a separate program to overwrite data, supplied as a part of MacAfee or Norton Utilities. Otherwise, the PC normal erasure routine keeps the data intact until overwritten.

Individual Access Controls

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner.

Insecure Internet Links

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of EKSG.

Encryption

Secure EKSG Sensitive information in accordance with the *Acceptable Encryption Standards*. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

One Time Password Authentication

One Time Password Authentication on Internet connections is accomplished by using a one time password token to connect to EKSG's internal network over the Internet. Contact your support organization for more information on how to set this up.

Physical Security

Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link

A Private Link is an electronic communications path that EKSG has control over its entire distance. For example, all EKSG networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer has established a private link. An ISDN or ADSL line to an employee's homes is a private link. EKSG also has established private links to other companies – trusted third parties for transactions processing and forwarding in a secure manner. Companies which EKSG has established private links to include all announced partner banks and third party switches/processor that EKSG has integrated to.

2.0 Audit Standards

Audit Vulnerability Scan Standards

2.1.0 Purpose

The purpose of this agreement is to set forth our agreement regarding network security scanning offered by an appropriate penetration testing services provider to the EKSG. The provider shall utilize [Approved Software](#) to perform electronic scans of EKSG's networks and/or firewalls or on any system at EKSG.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible security incidents ensure conformance to EKSG security policies
- Monitor user or system activity where appropriate.

2.2.0 Scope

This standard covers all computer and communication devices owned or operated by EKSG. This standard also covers any computer and communications device that are present on EKSG premises, but which may not be owned or operated by EKSG. The Penetration Testing Provider will not perform Denial of Service activities.

2.3.0 Standards

When requested, and for the purpose of performing an audit, consent to access needed will be provided to members of [The Penetration Testing Provider](#). EKSG hereby provides its consent to allow [The Penetration Testing Provider Auditors](#) to access its networks and/or firewalls to the extent necessary to allow The Penetration Testing Provider to perform the scans authorized in this agreement. EKSG shall provide protocols, addressing information, and network connections sufficient for [The Penetration Testing Provider](#) to utilize the software to perform network scanning.

This access may include:

- User level and/or system level access to any computing or communications device
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on EKSG equipment or premises
- Access to work areas (labs or test environments, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on EKSG networks.

2.4.1 Network Control.

If Client does not control their network and/or Internet service is provided via a second or third party, these parties are required to approve scanning in writing if scanning is to occur outside of the EKSG's LAN. By signing this agreement, all involved parties acknowledge that they authorize of [The Penetration Testing Provider Auditor](#) to use their service networks as a gateway for the conduct of these tests during the dates and times specified.

2.4.2 Service Degradation and/or Interruption. Network performance and/or availability may be affected by the network scanning. EKSG releases [The Penetration Testing Provider](#) of any and all liability for damages that may arise from network availability restrictions caused by the network scanning, unless such damages are the result [The Penetration Testing Provider's](#) gross negligence or intentional misconduct.

2.4.3 Client Point of Contact During the Scanning Period. EKSG shall identify in writing a person to be available if the result [The Penetration Testing Provider's](#) Scanning Team has questions regarding data discovered or requires assistance.

2.4.4 Scanning period. EKSG and [The Penetration Testing Provider](#) Scanning Team shall identify in writing the allowable dates for the scan to take place.

2.5.0 Enforcement

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

3.0 Acquisition Assessment Standards

3.1.0 Purpose

To establish IT responsibilities regarding corporate acquisitions, and define the minimum security requirements of an IT acquisition assessment.

3.2.0 Scope

This standards applies to all companies acquired by EKSG and pertains to all systems, networks, laboratories, test equipment, hardware, software and firmware, owned and/or operated by the acquired Government.

3.3.0 Standards

3.3.1 General

Acquisition assessments are conducted to ensure that a Government being acquired by EKSG does not pose a security risk to corporate networks, internal systems, and/or confidential/sensitive information. IT will provide personnel to serve as active members of the acquisition team throughout the acquisition process. The IT role is to detect and evaluate information security risk, develop a remediation plan with the affected parties for the identified risk, and work with the acquisitions team to implement solutions for any identified security risks, prior to allowing connectivity to EKSG's networks. Below are the minimum requirements that the acquired Government must meet before being connected to the EKSG's network.

3.3.2 Requirements

A. Hosts

1. All hosts (servers, desktops, laptops) will be replaced or re-imaged with a EKSG standard image.
2. Business critical production servers that cannot be replaced or re-imaged must be audited and a waiver granted by IT and Security & Risk units.
3. All PC based hosts will require EKSG approved virus protection before the network connection.

B. Networks

1. All network devices will be replaced or re-imaged with a EKSG standard image.
2. Wireless network access points will be configured to the EKSG standard.

3.3.3 Internet

1. All Internet connections will be terminated.
2. When justified by business requirements, air-gapped Internet connections require IT and Security & units' review and approval.

3.3.4 Remote Access

1. All remote access connections will be terminated.
2. Remote access to the production network will be provided by EKSG.

3.3.5 Labs

1. Lab (test environment) equipment must be physically separated and secured from non-lab areas.
2. The lab network must be separated from the corporate production network with a firewall between the two networks.
3. Any direct network connections (including analog lines, ADSL, ISDN lines, T1, etc.) to external customers, partners, etc., must be reviewed and approved by the Lab Security Group, LabSec within IT).
4. All acquired labs must meet with LabSec lab standards, or be granted a waiver by LabSec.
5. In the event the acquired networks and computer systems being connected to the corporate network fail to meet these requirements, the EKSG Head of IT must acknowledge and approve of the risk to EKSG's networks.

3.4.0 Enforcement

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

3.5.0 Definitions

Terms

Definitions

Business Critical Production Server A server that is critical to the continued business operations of the acquired Government.

4.0 Password Standards

4.1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of EKSG's entire corporate network. As such, all EKSG employees (including contractors and vendors with access to EKSG systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

4.2.0 Purpose

The purpose of this standard is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

4.3.0 Scope

The scope of this standards includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any EKSG facility, has access to the EKSG network, or stores any non-public EKSG information.

4.4.0 Standards

4.4.1 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the IT administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.

- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

4.4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at EKSG. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than fifteen characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
 - Names of family, pets, friends, co-workers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software.
 - The words "EKSG", "Lagos", "Hausa" or any derivation.
 - Birthdays and other personal information such as addresses and phone numbers.
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - Any of the above spelled backwards.
 - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#\$%^&*()_+|~-=\`{}[]:;'<>?,./)

- Are at least fifteen alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for EKSG accounts as for other non EKSG access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various EKSG access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account (if applicable).

Do not share EKSG passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential EKSG information.

Here is a list of "don't's":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Technology and/or Security & Risk Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to IT and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by IT or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions.

Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users

Access to the EKSG Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

4.5.0 Enforcement

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

4.6.0 Definitions

Terms

Definitions

Application Administration Account Any account that is for the administration of an application (e.g., Oracle database administrator, CMS administrator).

5.0 Remote Access Standards

5.1.0 Purpose

The purpose of this standards is to define standards for connecting to EKSG's network from any host. These standards are designed to minimize the potential exposure to EKSG from damages which may result from unauthorized use of EKSG resources. Damages include the loss of sensitive or Government confidential data, intellectual property, damage to public image, damage to critical EKSG internal systems, etc.

5.2.0 Scope

This standards applies to all EKSG employees, contractors, vendors and agents with a EKSG owned or personally-owned computer or workstation used to connect to the EKSG network. This standards applies to remote access connections used to do work on behalf of EKSG, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this standards include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

5.3.0 Standards

5.3.1 General

1. It is the responsibility of EKSG employees, contractors, vendors and agents with remote access privileges to EKSG's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to EKSG.
2. General access to the Internet for recreational use by immediate household members through the EKSG Network on personal computers is permitted for employees that have flat-rate services. The EKSG employee is responsible to ensure the family member does not violate any EKSG policies, does not perform illegal activities, and does not use the access for outside business interests. The EKSG employee bears responsibility for the consequences should the access be misused.

3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of EKSG's network:
 - a. *Acceptable Encryption Standards*
 - b. *Virtual Private Network (VPN) Standards*
 - c. *Wireless Communications Standards*
 - d. *Acceptable Use Standards*
4. For additional information regarding EKSG's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

3.3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Standards.
2. At no time should any EKSG employee provide their login or email password to anyone, not even family members.
3. EKSG employees and contractors with remote access privileges must ensure that their 3Lilne-owned or personal computer or workstation, which is remotely connected to EKSG's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. EKSG employees and contractors with remote access privileges to EKSG's corporate network must not use non-EKSG email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct EKSG business, thereby ensuring that official business is never confused with personal business.
5. Routers for dedicated ISDN lines configured for access to the EKSG network must meet minimum authentication requirements of CHAP.
6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
7. Frame Relay must meet minimum authentication requirements of DLCI standards.

8. Non-standard hardware configurations must be approved by Remote Access Services, and IT must approve security configurations for access to hardware.
9. All hosts that are connected to EKSG internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
10. Personal equipment that is used to connect to EKSG's networks must meet the requirements of EKSG-owned equipment for remote access.
11. Organizations or individuals who wish to implement non-standard Remote Access solutions to the EKSG production network must obtain prior approval from Remote Access Services and IT.

5.4.0 Enforcement

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

5.5.0 Definitions

Term	Definition
Cable Modem	Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.
CHAP	Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCIData Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital

data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into Linkserve or other Internet service provider (ISP). Being on a EKSG-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into EKSG's Network and an ISP, depending on packet destination.
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Frame Relay	A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone Government's network.
ISDN	There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.
Remote Access	Any access to EKSG's corporate network through a non-EKSG controlled network, device, or medium.
Split-tunneling	Simultaneous direct access to a non-EKSG network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into EKSG's corporate network via a VPN tunnel. VPN

Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

6.0 Internet Usage Standards

The Internet usage Standards applies to all Internet users (individuals working for EKSG, including permanent full-time and part-time employees, contract workers, temporary agency workers, business partners, and vendors) who access the Internet through the computing or networking resources. The EKSG's Internet users are expected to be familiar with and to comply with this standards, and are also required to use their common sense and exercise their good judgment while using Internet services.

6.1.0 Consequences of Violations

Violations of the *Internet usage Standards* will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination.

Additionally, EKSG may at its discretion seek legal remedies for damages incurred as a result of any violation. EKSG may also be required by law to report certain illegal activities to the proper enforcement agencies.

Before access to the Internet via EKSG's network is approved, the potential Internet user is required to read this Internet usage Standards and sign an acknowledgment form (located on the last page of this document). The signed acknowledgment form should be turned in and will be kept on file at the facility granting the access. For questions on the Internet usage Standards, contact the Information Technology (IT) Department.

6.2.0 USAGE THREATS

Internet connectivity presents EKSG with new risks that must be addressed to safeguard the facility's vital information assets. These risks include:

6.2.1 Inappropriate Use of Resources

Access to the Internet by personnel that is inconsistent with business needs results in the misuse of resources. These activities may adversely affect productivity due to time spent using or

"surfing" the Internet. Additionally, the Government may face loss of reputation and possible legal action through other types of misuse.

6.2.2 Misleading or False Information

All information found on the Internet should be considered suspect until confirmed by another reliable source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

6.3.0 INTERNET SERVICES

Access to the Internet will be provided to users to support business activities and only on an as-needed basis to perform their jobs and professional roles.

6.3.1 User Services

6.3.1.1 Internet Services Allowed

Internet access is to be used for business purposes only. Capabilities for the following standard Internet services will be provided to users as needed:

- E-mail -- Send/receive E-mail messages to/from the Internet (with or without document attachments).
- Navigation -- WWW services as necessary for business purposes, using a hypertext transfer protocol (HTTP) browser tool. Full access to the Internet; limited access from the Internet to dedicated Government public web servers only.
- File Transfer Protocol (FTP) -- Send data/files and receive in-bound data/files, as necessary for business purposes.
- Telnet -- Standard Internet protocol for terminal emulation. User Strong Authentication required for Internet initiated contacts into EKSG.

Management reserves the right to add or delete services as business needs change or conditions warrant.

All other services will be considered unauthorized access to/from the Internet and will not be allowed.

6.3.2 Request & Approval Procedures

Internet access will be provided to users to support business activities and only as needed to perform their jobs.

6.3.2.1 Request for Internet Access

As part of the Internet access request process, the employee is required to read both this Internet usage Standards and the associated Internet/Intranet Security Standards. The user must then sign the statements (located on the last page of each document) that he/she understands and agrees to comply with the policies. Users not complying with these policies could be subject to disciplinary action up to and including termination.

Standards awareness and acknowledgment, by signing the acknowledgment form, is required before access will be granted.

6.3.2.2 Approval

Internet access is requested by the user or user's manager submitting an **IT Access Request** form to the IT department along with an attached copy of a signed Internet usage Coverage Acknowledgment Form.

6.3.2.3 Removal of privileges

Internet access will be discontinued upon termination of employee, completion of contract, end of service of non-employee, or disciplinary action arising from violation of this standards. In the case of a change in job function and/or transfer the original access code will be discontinued, and only reissued if necessary and a new request for access is approved.

All user IDs that have been inactive for thirty (30) days will be revoked. The privileges granted to users must be reevaluated by management annually. In response to feedback from management, systems administrators must promptly revoke all privileges no longer needed by users.

6.4. USAGE POLICIES

6.4.1 Resource Usage

Access to the Internet will be approved and provided only if reasonable business needs are identified. Internet services will be granted based on an employee's current job responsibilities. If an employee moves to another business unit or changes job functions, a new Internet access request must be submitted within 5 days.

User Internet access requirements will be reviewed periodically by EKSG's IT departments to ensure that continuing needs exist.

6.4.2 Allowed Usage

Internet usage is granted for the sole purpose of supporting business activities necessary to carry out job functions. All users must follow the corporate principles regarding resource usage and exercise good judgment in using the Internet. Questions can be addressed to the IT Department.

Acceptable use of the Internet for performing job functions might include:

- Communication between employees and non-employees for business purposes;
- IT technical support downloading software upgrades and patches;
- Review of possible vendor web sites for product information;
- Reference regulatory or technical information.
- Research

6.4.3 Personal Usage

Using EKSG's computer resources to access the Internet for personal purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action up to and including termination.

All users of the Internet should be aware that the Government network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.

Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The

Government is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property

6.4.4 Prohibited Usage

Information stored in the wallet, or any consequential loss of personal property.

Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited.

EKSG also prohibits the conduct of a business enterprise, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libelous materials.

Other activities that are strictly prohibited include, but are not limited to:

- ☐ Accessing Government information that is not within the scope of one's work. This includes unauthorized reading of customer account information, unauthorized access of personnel file information, and accessing information that is not needed for the proper execution of job functions.
- ☐ Misusing, disclosing without proper authorization, or altering customer or personnel information. This includes making unauthorized changes to a personnel file or sharing electronic customer or personnel data with unauthorized personnel.
- ☐ Deliberate pointing or hyper-linking of Government Web sites to other Internet/WWW sites whose content may be inconsistent with or in violation of the aims or policies of the Government.
- ☐ Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law including without limitations international (foreign countries) export control laws and regulations.
- ☐ Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization. Assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.

- ☐ Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.
- ☐ Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libelous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
- ☐ Any form of gambling.

Unless specifically authorized under the provisions of section 4.3, the following activities are also strictly prohibited:

- ☐ Unauthorized downloading of any shareware programs or files for use without authorization in advance from the IT Department and the user's manager.
- ☐ Any ordering (shopping) of items or services on the Internet.
- ☐ Playing of any games.
- ☐ Forwarding of chain letters.
- ☐ Participation in any on-line contest or promotion.
- ☐ Acceptance of promotional gifts.

Bandwidth both within EKSG and in connecting to the Internet is a shared, finite resource. Users must make reasonable efforts to use this resource in ways that do not negatively affect other employees. Specific departments may set guidelines on bandwidth use and resource allocation, and may ban the downloading of particular file types.

If you have any questions about Acceptable Use, contact the IT Department

6.4.5 Software License

EKSG strongly supports strict adherence to software vendors' license agreements. When at work, or when Government computing or networking resources are employed, copying of software in a manner not consistent with the vendor's license is strictly forbidden. Questions regarding lawful versus unlawful copying should be referred to the IT Department for review or to request a ruling from the Legal and/or Compliance Department before any copying is done.

Similarly, reproduction of materials available over the Internet must be done only with the written permission of the author or owner of the document. Unless permission from the copyright owner(s) is first obtained, making copies of material from magazines, journals, newsletters, other publications and online documents is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

Using Government computer resources to access the Internet for personal purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action up to and including termination.

All users of the Internet should be aware that the Government network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.

Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The Government is not responsible for any loss of information.

6.4.6 Review of Public Information

All publicly-writeable directories on Internet-connected computers will be reviewed and cleared each evening. This process is necessary to prevent the anonymous exchange of information inconsistent with Government business. Examples of unauthorized public information include pirated information, passwords, credit card numbers, and pornography.

6.4.7 Expectation of Privacy

6.4.7.1 Monitoring

Users should consider their Internet activities as periodically monitored and limit their activities accordingly.

Management reserves the right to examine E-mail, personal file directories, web access, and other information stored on Government computers, at any time and without notice. This examination ensures compliance with internal policies and assists with the management of Government information systems.

6.4.7.2 E-mail Confidentiality

Users should be aware that clear text E-mail is not a confidential means of communication. The Government cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Users should also be aware that once an E-mail is transmitted it may be altered. Deleting an E-mail from an individual workstation will not eliminate it from the various systems across which it has been transmitted.

6.4.8 Maintaining Corporate Image

6.4.8.1 Representation

When using Government resources to access and use the Internet, users must realize they represent the Government. Whenever employees state an affiliation to the Government, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the Government". Questions may be addressed to the IT Department.

6.4.8.2 Government Materials

Users must not place Government material (examples: internal memos, press releases, product or usage information, documentation, etc.) on any mailing list, public news group, or such service. Any posting of materials must be approved by the employee's manager and the Corporate Services department and will be placed by an authorized individual.

6.4.8.3 Creating Web Sites

All individuals and/or business units wishing to establish a WWW home page or site must first develop business, implementation, and maintenance plans. Formal authorization must be obtained through the IT Department and Compliance Unit. This will maintain publishing and content standards needed to ensure consistency and appropriateness.

In addition, contents of the material made available to the public through the Internet must be formally reviewed and approved before being published. All material should be submitted to the General Manager and/or Head of Corporate Services for initial approval to continue. All Government pages are owned by, and are the ultimate responsibility of, the Corporate Service

Department.

All Government web sites must be protected from unwanted intrusion through formal security measures which can be obtained from the IT department.

6.4.9 Periodic Reviews

6.4.9.1 Usage Compliance Reviews

To ensure compliance with this standards, periodic reviews will be conducted. These reviews will include testing the degree of compliance with usage policies.

6.4.9.2 Standards Maintenance Reviews

Periodic reviews will be conducted to ensure the appropriateness and the effectiveness of usage policies. These reviews may result in the modification, addition, or deletion of usage policies to better suit Government information needs.

6.5. REFERENCES

6.5.1 Points of Contact

If you need assistance regarding the following topics related to Internet usage, contact the IT Department for additional assistance:

Corporate Level:
Acceptable Use
Public Representation
Web Site
Legal Department
Corporate Services Department
Corporate Principles
Regional Level:
Access or Connection Problems

6.6. INTERNET USAGE COVERAGE ACKNOWLEDGMENT FORM

After reading these standards, please sign the coverage form and submit it to your facility's ICT department or granting facility's ICT department for filing.

By signing below, the individual requesting Internet access through Government computing resources hereby acknowledges receipt of and compliance with the Internet Usage Standards. Furthermore, the undersigned also acknowledges that he/she has read and understands these standards before signing this form.

Internet access will not be granted until this acknowledgment form is signed by the individual's manager. After completion, the form is filed in the individual's human resources file (for permanent employees), or in a folder specifically dedicated to Internet access (for contract workers, etc.), and maintained by the IT department. These acknowledgment forms are subject to internal audit.

7.0 Internet Demilitarized Zone (DMZ) Equipment Standards

7.1.0 Purpose

The purpose of these standards is to define standards to be met by all equipment owned and/or operated by EKSG located outside EKSG's corporate Internet firewalls. These standards are designed to minimize the potential exposure of EKSG from the loss of sensitive or Government confidential data, intellectual property, damage to public image etc., which may follow from unauthorized use of EKSG's resources.

Devices that are Internet facing and outside the EKSG's firewalls are considered part of the "demilitarized zone" (DMZ) and are subject to this standards. These devices (network and host) are particularly vulnerable to attack from the Internet since they reside outside the corporate firewalls.

The standards define the following standards:

- Ownership responsibility
- Secure configuration requirements
- Operational requirements
- Change control requirement

7.2.0 Scope

All equipment or devices deployed in a DMZ owned and/or operated by EKSG (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by EKSG, must follow this standards.

This standard also covers any host device outsourced or hosted at external/third-party service providers, if that equipment resides in the "EKSGng.com" domain or appears to be owned by EKSG.

All new equipment which falls under the scope of this standard must be configured according to the referenced configuration documents, unless a waiver is obtained from IT. All existing and future equipment deployed on EKSG's un-trusted networks must comply with this standard.

7.3.0 Standards

7.3.1. Ownership and Responsibilities

Equipment and applications within the scope of this standard must be administered by support groups approved by IT for DMZ system, application, and/or network management.

Support groups will be responsible for the following:

- Equipment must be documented in the corporate wide enterprise management system. At a minimum, the following information is required:
 - Host contacts and location.
 - Hardware and operating system/version.
 - Main functions and applications.
 - Password groups for privileged passwords.
- Network interfaces must have appropriate Domain Name Server records (minimum of A and PTR records).
- Password groups must be maintained in accordance with the corporate wide password management system/process.
- Immediate access to equipment and system logs must be granted to members of IT upon demand, per the *Audit Standards*.
- Changes to existing equipment and deployment of new equipment must follow; and corporate governance or change management processes/procedures.

To verify compliance with this standard, IT and Compliance Unit will periodically audit DMZ equipment per the *Audit Standards*.

7.3.2. General Configuration Standards

All equipment must comply with the following configuration standards:

- Hardware, operating systems, services and applications must be approved by IT as part of the pre-deployment review phase.
- Operating system configuration must be done according to the secure host and router installation and configuration standards (Approved Government standard).

- All patches/hot-fixes recommended by the equipment vendor and IT must be installed. This applies to all services installed, even though those services may be temporarily or permanently disabled. Administrative owner groups must have processes in place to stay current on appropriate patches/hot-fixes.
- Services and applications not serving business requirements must be disabled.
- Trust relationships between systems may only be introduced according to business requirements, must be documented, and must be approved by IT and/or Security & Risk units.
- Services and applications not for general access must be restricted by access control lists.
- Insecure services or protocols (as determined by IT) must be replaced with more secure equivalents whenever such exist.
- Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks. Where a methodology for secure channel connections is not available, one-time passwords (DES/SofToken) must be used for all access levels.
- All host content updates must occur over secure channels.
- Security-related events must be logged and audit trails saved to IT Security-approved logs. Security-related events include (but are not limited to) the following:
 - User login failures.
 - Failure to obtain privileged access.
 - Access standards violations.
- IT Security will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

7.3.3. New Installations and Change Management Procedures

All new installations and changes to the configuration of existing equipment and applications must follow the following policies/procedures:

- New installations must be done via the *DMZ Equipment Deployment Process*.
- Configuration changes must follow the Corporate Change Management (CM) Procedures.

- IT must be invited to perform system/application audits prior to the deployment of new services.
- IT must be engaged, either directly or via CM, to approve all new deployments and configuration changes.

7.3.4. Equipment Outsourced to External Service Providers

The responsibility for the security of the equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures documented. Contracting departments are responsible for third party compliance with this standard.

7.4.0 Enforcement

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

External service providers found to have violated this standard may be subject to financial penalties, up to and including termination of contract.

7.5.0 Definitions

Terms	Definitions
DMZ (de-militarized zone)	Any un-trusted network connected to, but separated from, EKSG's corporate network by a firewall, used for external (Internet/partner, etc.) access from within EKSG, or to provide information to external parties. Only DMZ networks connecting to the Internet fall under the scope of this standard.
Secure Channel	Out-of-band console management or channels using strong encryption according to the <i>Acceptable Encryption Standards</i> . Non-encrypted channels must use strong user authentication (one-time passwords).

Un-Trusted Network

Any network firewalled off from the corporate network to avoid impairment of production resources from irregular network traffic (lab networks), unauthorized access (partner networks, the Internet etc.), or anything else identified as a potential threat to those resources.

8.0 Wireless Communications Standards

8.1.0 Overview

The purpose of this standard is to secure and protect the information assets owned by EKSG. EKSG provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. EKSG grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This standards specifies the conditions that wireless infrastructure devices must satisfy to connect to EKSG network. Only those wireless infrastructure devices that meet the standards specified in this standards or are granted an exception by the IT and/or Security & Risk Departments are approved for connectivity to a EKSG's network.

8.2.0 Scope

All employees, contractors, consultants, temporary and other workers EKSG, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of EKSG must adhere to this standard. This standards applies to all wireless infrastructure devices that connect to a EKSG network or reside on a EKSG site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and personal digital assistants (PDAs). This includes any form of wireless communication device capable of transmitting packet data.

The IT and/or Security & Risk Departments or units must approve exceptions to this standards in advance.

8.3.0 Standards Statement

8.3.1 General Network Access Requirements

All wireless infrastructure devices that reside at a EKSG site and connect to a EKSG network, or provide access to information classified as EKSG Confidential, EKSG Highly Confidential, or EKSG Restricted must:

- Abide by the standards specified in the Wireless Communication Standard.
- Be installed, supported, and maintained by an approved support team.
- Use EKSG approved authentication protocols and infrastructure.
- Use EKSG approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.

8.3.2 Lab (or Test Environment) and Isolated Wireless Device Requirements

All lab wireless infrastructure devices that provide access to EKSG Confidential, EKSG Highly Confidential, or EKSG Restricted information must adhere to section 0. Lab and isolated wireless devices that do not provide general network connectivity to the EKSG network must:

- 3.21 Be isolated from the corporate network (that is it must not provide any corporate connectivity) and comply with the DMZ Lab Security Standards or the Internal Lab Security Standards.
- 3.22 Not interfere with wireless access deployments maintained by other support organizations.

- **3.3 Home Wireless Device Requirements**

- 3.31 Wireless infrastructure devices that provide direct access to the EKSG corporate network, must conform to the Home Wireless Device Requirements as detailed in the Wireless Communication Standard.
- 3.32 Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the EKSG corporate network. Access to the EKSG corporate network through this device must use standard remote access authentication.

8.4.0 Enforcement

An employee found to have violated this standard may be subject to disciplinary action, up to and including termination of employment. A violation of this standard by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with EKSG

8.5.0 Definitions

Term	Definition
EKSG's network	A wired or wireless network including indoor, outdoor, and alpha networks that provide connectivity to corporate services.
Corporate connectivity	A connection that provides access to a EKSG's network.
Enterprise Class Teleworker (ECT)	An end-to-end hardware VPN solution for teleworker access to the EKSG's network.
Information assets	Information that is collected or produced and the underlying hardware, software, services, systems, and technology that is necessary for obtaining, storing, using, and securing that information which is recognized as important and valuable to an organization.
MAC address	The MAC (Media Access Control) address is a hardware number that uniquely identifies each node on a network and is required for every port or device that connects to the network.

9.0 Risk Assessment Standards

EKSG's Enterprise Risk Assessment Standards

9.1.0 Purpose

To empower EKSG to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

9.2.0 Scope

Risk assessments can be conducted on any entity within EKSG or any outside entity that has signed a *Third Party Agreement* with EKSG. RAs can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

9.3.0 Standards

The execution, development and implementation of remediation programs are the joint responsibility of EKSG's IT, Risk and Compliance departments and the department responsible for the systems areas being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the EKSG's Enterprise Risk Assessment Team in the development of a remediation plan.

9.4.0 Risk Assessment Process

For additional information, go to the Risk Assessment Process.

9.5.0 Enforcement

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

9.6.0 Definitions

Terms

Definitions

Entity Any business unit, department, group, or third party, internal or external to EKSG, responsible for maintaining EKSG's assets.

Risk Those factors that could affect confidentiality, availability, and integrity of EKSG's key information assets and systems. EKSG's IT department is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

10.9 Router Security Standards

10.1.0 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 EKSG.

10.2.0 Scope

All routers and switches connected to EKSG production networks are affected. Routers and switches within internal, secured labs are not affected. Routers and switches within DMZ areas fall under the *Internet DMZ Equipment Standards*.

10.3.0 Standards

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 authentications.
2. The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.
3. Disallow the following:
 - a. IP directed broadcasts
 - b. Incoming packets at the router sourced with invalid addresses such as RFC1918 address
 - c. TCP small services
 - d. UDP small services
 - e. All source routing
 - f. All web services running on router
4. Use corporate standardized SNMP community strings.
5. Access rules are to be added as business needs arise.
6. The router must be included in the corporate enterprise management system with a designated point of contact.
7. Each router must have the following statement posted in clear view:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.

You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this standards may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device."

8. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH is the preferred management protocol.

10 . 4.0 Enforcement

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

10 . 5.0 Definitions

Terms	Definitions
Production Network	The "production network" is the network used in the daily business of EKSG. Any network connected to the corporate backbone, either directly or indirectly, which lacks an intervening firewall device. Any network whose impairment would result in direct loss of functionality to EKSG employees or impact their ability to do work.
Lab Network	A "lab network" is defined as any network used for the purposes of testing, demonstrations, training, etc. Any network that is stand-alone or firewalled off from the production network(s) and whose impairment will not cause direct loss to EKSG nor affect the production network.

11.9 Server Security Standards

11.1.0 Purpose

The purpose of this standard is to establish standards for the base configuration of internal server equipment that is owned and/or operated by EKSG. Effective implementation of this standard will minimize unauthorized access to EKSG proprietary information and technology.

11.2.0 Scope

This standards applies to server equipment owned and/or operated by EKSG, and to servers registered under any EKSG-owned internal network domain.

This standards is specifically for equipment on the internal EKSG network. For secure configuration of equipment external to EKSG on the DMZ, refer to the *Internet DMZ Equipment Standards*.

11.3.0 Standards

11.3.1 Ownership and Responsibilities

All internal servers deployed at EKSG must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by IT. Operational groups should monitor configuration compliance and implement an exception standards tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by IT.

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
 - Server contact(s) and location, and a backup contact
 - Hardware and Operating System/Version
 - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.

- Configuration changes for production servers must follow the appropriate change management procedures.

11.3.2 General Configuration Guidelines

- Operating System configuration should be in accordance with approved IT guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

11.3.3 Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
 - All security related logs will be kept online for a minimum of 1 week.
 - Daily incremental tape backups will be retained for at least 1 month.
 - Weekly full tape backups of logs will be retained for at least 1 month.
 - Monthly full backups will be retained for a minimum of 2 years.

- Security-related events will be reported to IT, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
 - Port-scan attacks
 - Evidence of unauthorized access to privileged accounts
 - Anomalous occurrences that are not related to specific applications on the host.

11.3.4 Compliance

- Audits will be performed on a regular basis by authorized unit(s) or department(s) within EKSG or appointed third party auditor.
- Audits will be managed by the internal audit group or Compliance or Security & Risk and IT, in accordance with the *Audit Standards*. IT will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

11.4.0 Enforcement

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

11.5.0 Definitions

Term	Definition
DMZ	De-militarized Zone. A network segment external to the corporate production network.
Server	For purposes of this standard, a Server is defined as an internal EKSG Server. Desktop machines and Lab equipment are not relevant to the scope of this standard.

APPENDIX 4

1.0 Third Party (3rd Party) Connectivity Standards (Extranet Standard)

1.1 Purpose

This document describes the standards under which third party organizations connect to EKSG networks for the purpose of transacting business related to EKSG.

1.2 Scope

Connections between third parties that require access to non-public EKSG resources fall under this standards, regardless of whether a Telco circuit (such as frame relay, ADSL or ISDN) or VPN technology is used for the connection. Connectivity to third parties such as the Internet Service Providers (ISPs) that provide Internet access for EKSG or to the Public Switched Telephone Network does NOT fall under this standards.

1.3 Standards

1.3.1 Pre-Requisites

1.3.2 Security Review

All new extranet connectivity will go through a security review with the Information Technology and/or Risk & Security units. The reviews are to ensure that all access matches the business requirements in a best possible way, and that the principle of least access is followed.

1.3.3 Third Party Connection Agreement

All new connection requests between third parties and EKSG require that the third party and EKSG representatives agree to and sign the *Third Party Agreement*. This agreement must be signed by an appropriate Head of Department or authorized officer of the Sponsoring Organization (**Department or Units**) as well as a representative from the third party who is legally empowered to sign on behalf of the third party. The signed document is to be kept on file with the relevant extranet group. Documents pertaining to connections into EKSG labs (or test environment) are to be kept on file with the [name of team responsible for security of labs – where applicable].

1.3.4 Business Case

All production extranet connections must be accompanied by a valid business justification, in writing, that is approved by a project manager in the extranet group. Lab (or test environment) connections must be approved by the Head of Information Technology Department and/or of Security & Risk. Typically this function is handled as part of the *Third Party Agreement*.

1.3.5 Point Of Contact

The Sponsoring Organization (Department or Unit) must designate a person to be the Point of Contact (POC) for the Extranet connection. The POC acts on behalf of the Sponsoring Organization, and is responsible for those portions of this standards and the *Third Party Agreement* that pertain to it. In the event that the POC changes, the relevant extranet Organization must be informed promptly.

1.4 Establishing Connectivity

Sponsoring Organizations (Departments or Units) within EKSG that wish to establish connectivity to a third party are to file a new site request with the proper extranet group. The extranet group will engage IT and/or Security & Risk to address security issues inherent in the project. If the proposed connection is to terminate within a lab (or test environment) at EKSG, the Sponsoring Organization must engage the officer responsible for security of labs/test environment. The Sponsoring Organization must provide full and complete information as to the nature of the proposed access to the extranet group and IT, as requested.

All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review. In no case will EKSG rely upon the third party to protect EKSG's network or resources.

1.5 Modifying or Changing Connectivity and Access

All changes in access must be accompanied by a valid business justification, and are subject to security review. Changes are to be implemented via corporate change management process. The Sponsoring Organization is responsible for notifying the extranet management group and/or IT when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

1.6 Terminating Access

When access is no longer required, the Sponsoring Organization within EKSG must notify the extranet team responsible for that connectivity, which will then terminate the access. This may mean a modification of existing permissions up to terminating the circuit, as appropriate. The extranet and lab security teams must conduct an audit of their respective connections on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the needs of the connection. Connections that are found to be depreciated, and/or are no longer being used to conduct EKSG business, will be terminated immediately. Should a security incident or a finding that a circuit has been depreciated and is no longer being used to conduct EKSG business necessitate a modification of existing permissions, or termination of connectivity, IT and/or the extranet team will notify the POC or the Sponsoring Organization of the change prior to taking any action.

1.7 Enforcement

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

1.8 Definitions

Terms	Definitions
Circuit	For the purposes of this standards, circuit refers to the method of network access, whether it's through traditional ISDN, Frame Relay etc., or via VPN/Encryption technologies.
Organization	Means any department or unit within EKSG as a Government
Sponsoring Organization	The EKSG organization who requested that the third party have access into EKSG.
Third Party	A business that is not a formal or subsidiary part of EKSG.