

Rwanda Information Technology Authority



Technical Standards and Guidelines for E-Government – Final Report

Annexure A

Security Policy Guidelines

Feb - 2006

Prepared by :



Techno Brain (U) Ltd
Unit 13/14, Metropole House
Entebbe Road, PO Box 33339,
Kampala, Uganda
Email: info@technobrainuganda.info
Tel: 256-41-257987; 0312-263066/7
Fax: 256-41-347078

Annexure A: Security Policy Guidelines

Table of contents

1	Management Summary.....	3
1.1	Components	3
1.2	Audience	3
1.3	Assumptions	3
1.4	Salient features.....	4
2	Policy Guidelines.....	5
2.1	Components of the Policy.....	5
2.1.1	Information Security Management	5
2.1.2	Access Control Policy	5
2.1.3	Disaster Recovery Policy	6
2.1.4	Education, Training, Awareness Policy.....	6
2.1.5	Individual Use Policy.....	6
2.1.6	Network Security Policy	7
2.1.7	Security Breaches and Incident Reporting Policy	7
2.2	Setting up Security Regimes within agencies	7
3	Information Security Management	8
3.1	Identify Information Assets	8
3.2	Information Assets Types.....	8
3.3	Information Asset Repository	9
3.4	Information Asset Classification	9
3.4.1	Assigning Values to Assets	9
3.4.2	Classification on basis of threat assessment.....	12
3.4.3	Asset Classification Summary	13
3.5	Risk Analysis.....	15
3.5.1	Calculating the Loss Impact	15
3.5.2	Calculating the Value.....	16
3.5.3	Threats and Risks to Assets.....	17
3.5.4	Safeguards and Assets.....	19
3.6	How to do a Business Impact Analysis.....	22
3.6.1	How to identify information assets:.....	22
3.6.2	How to determine loss impact of an asset	22
3.6.3	How to calculate the value of an asset	23
3.6.4	How to identify threats/ risks to assets.....	32
3.6.5	How to safeguard your assets	32
4	Security Management Team	36
5	Creating an Awareness Program	45
5.1	What is ISS Awareness?.....	45
5.1.1	What is an Awareness Program?.....	46
5.1.2	What makes up an Awareness Program	49
5.1.3	Awareness Materials.....	50
6	Incident programs	53
6.1	What is an Incident Program?	53
6.1.1	Evidence	56
6.1.2	Incident Response.....	57
6.1.3	Investigating Incidents	58
6.1.4	Incident Reporting Form	59
6.1.5	Enforcement	59
6.1.6	Incident Handling.....	59
6.1.7	Implementing an Incident Program.....	61
6.1.8	Point of Contact Information	64

1 Management Summary

Background

Computers have increased dependence on information systems and they are now integral in all organizational operations. However, terrorism and sustained attacks from hostile quarters have made Information Systems Security (ISS) extremely important to any organization (and more so Governments) worldwide.

ISS is much more than computer system security. It is the process of protecting all intellectual property of an organization. Information takes many forms – what is stored on computers is just one form of intellectual property; but it can also be transmitted across networks, printed or written on paper, and spoken in conversations. Information and information technology systems are assets of vital importance to the institutions and government agencies and affects citizens and the security of the country.

It is the purpose of this document is to guide security professions implement an ISS program throughout the Rwandan Government. It provides the instruction and materials necessary to roll out an awareness program and publish a set of security policy and procedures. It is independent of any technology, but provides a template, which can be filled up with relevant details by various agencies.

1.1 Components

The following components of an ISS program have been addressed in this document:

- Security Policies and Procedures
- Asset Risk Assessment
- Security Tools and Materials
- Security Management Team
- Employee Awareness Program
- Employee Incident Response

1.2 Audience

The proposed users of this document are

- Security experts
- Users
- IT administrators

1.3 Assumptions

Implementers of this policy guide are expected to have:

- Knowledge of Security Management
- Knowledge of MS Office products

Annexure A: Security Policy Guidelines

1.4 Salient features

This document provides a step-by-step procedure that can be adapted to suit individual needs of agencies. Agencies should categorize the information depending on the criticality and need for protection and take the appropriate actions as suggested by this template. This is not a hard & fast rule and agencies are free to improve on the suggestions made here and ideally share these enhancements with other agencies in the Government.

2 Policy Guidelines

Every agency must define its own Information Security policy. This policy defines the goals of protecting property rights while not hindering the free flow of information. The policy shall define the information sources (suppliers) and sinks (consumers), define levels of security, access and modification rights; archival and physical protection of information resources, etc.

2.1 Components of the Policy

The key components of any security policy that must be addressed are enumerated below. Agencies are free to add additional policy components to suit individual needs.

2.1.1 Information Security Management

Scope: all systems that gather, generate, and store data.

- What is defined as information; who are the owners; how critical and sensitive the information is
- Define levels of security commensurate with the value of the information
- Target audience authorized to use or to view the information
- Authority to create, modify and destroy the information
- Archival needs of the information resource
- Information security programs that provide reasonable protection against unauthorized access, disclosure, modification, or destruction, as well as to assure the availability, integrity, utility, authenticity, and confidentiality of information.

2.1.2 Access Control Policy

Scope: all systems that gather, generate, and store data; physical data stores, offices and facilities;

Once the information assets and their security levels are defined, an access control mechanism must be put in place to ensure the security of the Information. Access Control protects information by managing access to all entry and exit points, (both logical and physical). This component covers:

- Perimeter security, firewalls, anti-virus and anti Spam / anti Ad-ware applications, setting up of demilitarized zones, etc. Physical security can also mean access control devices, monitoring entry and exit of personnel from / to restricted areas, close-circuit cameras and video recording, etc.
- Logical security restricts access by means of login and passwords, smart cards, biometric (e.g. finger print authentication), etc.

Overall, the system must ensure against unauthorized access to sensitive information on any governmental facility, network, or application. These measures ensure that only authorized users, as determined by each governmental entity, have access to specific computer resources, networks, data, reports and applications.

Annexure A: Security Policy Guidelines

2.1.3 Disaster Recovery Policy

Every agency must have a disaster recovery plan that at the very least identifies and militates against risks to critical systems and sensitive information in the event of a disaster. Disasters could be natural or deliberate, but the plans, procedures and human resources to quickly, effectively and efficiently recover from the disaster must be in place. In case of a disaster, the agency must be able to quickly setup an alternative site from where to operate and resume operations in the quickest and least disruptive manner possible. System disaster recovery procedures and plans are usually a subset of the organizational disaster recovery plans.

2.1.4 Education, Training, Awareness Policy

Security policies, rules, guidelines and procedures are as good as the people who implement them, not only at an administrative level, but also at the level of ordinary users. All users need to be trained on the components of the policy and secure use of the information assets. A minimal requirement of the policy is given below:

- These policies and procedures will be communicated to all employees and other users (e.g. the ones logging onto the agency website or suppliers tendering for a service).
- The information security policy and procedures will be available for reference and review by employees, contractors, agents acting on behalf of the agency and all others in a position to impact the security and integrity of the information assets of the agency.
- A program to maintain effective awareness of information security policy, standards, and acceptable practices will exist.
- Persons responsible for information technology resources must have adequate training on implementing proper security controls for the equipment, software, and networks under their control.
- Training will be an ongoing task with refresher trainings held at periodic intervals and as part of the induction training for new recruits
- At all times, adequate materials for training on the Security Policies of the agency will be available with it

2.1.5 Individual Use Policy

- By and large the intellectual assets and resources of the state or agency should be used in a judicious manner, for facilitating official tasks.
- Use of Internet, e-mail and other official resources for personal use must be curtailed as far as possible.
- All users must ensure that they do not indulge in any activity that does not befit the dignity or stature of their office or cause embarrassment to the organisation
- Individuals should be restricted from installing any kind of unauthorized software, music and other content that could be construed as illegal or could cause the organisation to pay penalties or fines or face legal actions
- Any individual violating this policy must face appropriate disciplinary action
- Periodic audits will be undertaken to ensure compliance

Annexure A: Security Policy Guidelines

2.1.6 Network Security Policy

- All agencies and institutions shall manage networks in a manner that insures their proper use, prevents unauthorized access or usage, maintains availability and protects the security of information resources.
- All agencies and institutions shall establish controls that are commensurate to the security needs of the information and computer resources on the network, as defined in the security levels for the identified resource.
- There must be a clear boundary between data accessible to the public and the production databases used within the agencies. Under no circumstances should production databases be exposed directly to connectivity over the Internet
- All agencies should also ensure that their network is not the cause of harm to users of and information stored on other networks connected to them
- Internet and intranet sites must be protected from intrusion so that an unauthorized individual cannot alter data and information or compromise the integrity of the government networks.
- User IDs and passwords or other unique identifier must further protect intranet sites so that access by unauthorized individuals is not allowed.
- The policy and standards set forth in the Individual Use and Access Control policies will apply.

2.1.7 Security Breaches and Incident Reporting Policy

- All agencies must prepare procedures for monitoring, investigating, and reporting security breaches and incidents.
- A hierarchy within Government spanning across various ministries and headed by a representative of the Ministry of Defense will be created to monitor the security apparatus within the Government
- This agency shall create a reporting procedure to ensure that security breaches get reported and addressed at appropriate level commensurate with the severity of the breach
- Security breaches shall be investigated promptly and documented. If criminal action is suspected, the agency or institution affected must contact the security agency and appropriate law enforcement and investigative authorities as quickly as possible.
- The policies and standards pertaining to access controls, acceptable use, education and network security shall apply.

2.2 Setting up Security Regimes within agencies

The following steps have been suggested while setting up a security policy and framework within agencies.

- Create an appropriate Security Policy based on the template given above
- Assemble a Security Team
- Conduct Business Impact Analysis
- Create the appropriate rules and classification of Information Resources
- Publish the Procedures and Rules
- Implement an Training / Awareness Program
- Implement an Incident Reporting Program
- Periodically audit security procedures and preparedness

3 Information Security Management

3.1 Identify Information Assets

Information assets are those resources that store, transport, create, use, or are information. These assets are those that add value to the organization or whose loss would reduce value to the organization.

In order to know what information you need to protect and how you are going to protect it, you must identify your information assets. A complete inventory is required to know what the organization requires for the ISS program. All information resources must be accounted for even if they are a low priority, low risk, or easy to replace.

3.2 Information Assets Types

Several types of assets can be classified under Information Technology. Some examples are:

- Platform
- Applications
- General Software
- Hardware
- Communications

Platform

The platform hosts a number of applications and a platform level security regime will protect all applications and data within the system. This regime is suitable for most users as often data residing in a machine usually has similar security characteristics – e.g. servers will have mission critical enterprise level data (possibly hosted in multiple applications); user desktops will have data relevant to the respective user but probably not of much importance to the organisation as a whole, and so on. Safeguarding assets at the platform level means that all the assets are given the same level of security and will have the same controls on access and distribution.

Applications

Different applications usually have different levels of security; a database system might have certain information that is accessible to all whereas a mail server will have various mailboxes that are to be accessed individually or possibly to closed user groups. To complicate matters further, a mail server may contain a global address book that is available for all to use. Similarly a payroll application needs greater security than (say) a leave application system.

Applications include both the data and the programs that run the application. All applications should be grouped here regardless if the software is purchased, rented, in-house developed, or third party.

General Software

All users use system software directly (e.g. Word) or indirectly through other applications (e.g. a database system). Security for use of these is often granted but administrative tasks and permissions are often tightly controlled

Annexure A: Security Policy Guidelines

Hardware

This hardware includes all processors (laptops, PCs, servers, etc.), printers, UPS, tape drives, storage drives, and all other equipment. Access to hardware (physical or logical) has to be defined and controlled.

Communications

All communication points need to be safeguarded. This category considers modems, communication lines, switches, routers, bridges, networks, etc

3.3 Information Asset Repository

The information repository must contain information about the network, network diagrams, what resources are hosted where, security level, etc. Typically the following information needs to be gathered for each asset:

- Name or identification
- Asset Inventory number
- Physical location
- Size in MB
- Number of users
- Primary Owner (agency)
- User agencies
- Vendor contact
- Service contact
- Backup location (in case of software applications or data)
- Local administrator
- Classification as explained below

Each application and general software asset can be assigned an owner. Accountability helps ensure that adequate security protection is maintained. The owner is responsible for evaluating, classifying, and protecting the asset. The implementation of the safeguards may be delegated, but the owner of the asset is responsible for protecting it. The owner can be a technical, business, or user resource.

3.4 Information Asset Classification

3.4.1 Assigning Values to Assets

Once the information assets have been identified, they must each be given a value or evaluation of the assets worth.

Different methods can be used to value assets. You can give the asset the value of simple replacement, but obviously several assets are irreplaceable. The value given can be any except that it must be followed consistently across all assets. The asset valuation is done with the goal of the process in mind, that is, to define assets in terms of a hierarchy of importance or criticality, the relative value of the assets becomes more important than placing the "correct" value on them.

Annexure A: Security Policy Guidelines

Generally, assets can be valued based on the impact and consequence to the organization. Assigning value depends on its loss to the Government (and hence the Nation), and how much of the organization relies on it. Value can be based on loss.

The value of an asset does not change because of good backup and recovery procedures. These are merely means of protecting valuable assets. All protection mechanisms are "removed" when calculating values.

Classification may be quantitative or qualitative. Quantitative approaches are widely used, but require more extensive research in getting to exact figures and balancing totals. It is often associated with measuring in terms of dollars or Francs and attempts to assign independently, objective numeric values (ex. monetary) to the components of the analysis. Quantitative classification usually requires precise figures such as product implementation and customization costs, etc.

Qualitative classification relies on less accurate figures but is usually equally effective. Some of the qualitative classifications commonly used are:

- Size (asset size in MB): the larger the system, the more valuable it is deemed to be
- No of users: the more the number of users, the more useful (and hence valuable) the asset

Working with a qualitative approach means you should not attempt to assign numeric values to the exact dollar or Franc. Qualitative approaches are often associated with measuring in terms of quality as indicated through a scale or ranking. It relies on scenarios and is subjective. As long as you are consistent and measure all assets using the same strategy, then the exact figure does not matter. Qualitative values can be imparted on a grade of 1:10 or 1:100 (say)

E.g. of qualitative classification of database applications

Size in MB	Classification - grade 1:100
25000+	100
10000+	80
5000+	60
2500+	40
1000+	20
< 1000	10

Number of Users	Classification - grade 1:100
100+	100
75+	80
50+	50
25+	25
10+	20
< 10	10

Qualitative valuations are relative and the valuation is simply a number that defines how much more valuable an asset is vis-à-vis another. This approach is just as effective as the quantitative approach.

Annexure A: Security Policy Guidelines

Assigning classifications determines day-to-day practices with information: how it is handled, who handles it, how it is transported, stored, who has access, where it can go, and such. You can use classification labels if you wish to follow information in whatever form / media it is transported – printed, electronic, or on a display screen. Once a data classification system has been adopted, it is very expensive and difficult to change to another system.

The owner of the asset in association with the proposed security agency should be the one that determines the sensitivity or classification.

Points to be considered while preparing the classifications:

Sensitivity of the data	This is the leading factor and should consider disclosure, damage, and loss of information and its impact on the business operations.
Regulated / legal and contractual obligations and penalties	What is the minimum level of classification required to which the law or contract applies? E.g. an official secrecy act may be applicable to the asset
Standards and guidelines	Are there any compliance standards to be adhered to? This will be particularly useful while acquiring new assets
Information lifecycle	What are the effects of the classification over time? In particular with disclosure, the importance can change over time. e.g. The closer to being made public the lower the classification.
Confidentiality	Describes the impact from disclosure and the protection of sensitive information.
Integrity	Reflects the severity of the damage that could be caused to the accuracy and completeness of the information and processing methods.
Availability	Urgency of the information and the systems that use it. Usually public documents are most accessible and vice versa
Non-repudiation	Proving transfer and receipt of un-reproducible electronic transaction

Annexure A: Security Policy Guidelines

3.4.2 Classification on basis of threat assessment

Information has to be then classified under various categories based on its criticality to the Government. This classification closely mimics the physical security given to paper documents and other similar information. Every ministry and agency will have some information that is classified under "Highly sensitive" while some other bits of information could be open and available to all. Some ministries will have major portion of their information classified under "Highly sensitive" or "Highly restricted" e.g. Defense; others, like Health may have most of the data available for public use. Even so, Defense would have some unclassified Information (e.g. Information for applicants for recruitment to the armed forces) and so on.

4 classifications under this scheme have been suggested. These are as under:

Security Level	Classification - grade 1:100
Highly restricted	100
Confidential	80
Internal use only	50
Unclassified / Public domain	1

HIGHLY RESTRICTED is for the most sensitive information intended strictly for use within the organization and controlled / issued under special rules to specific personnel. It is highly critical and demands the highest possible security.

Examples: Troop locations; troop movement; annual government budgetary figures prior to announcement of the budget

CONFIDENTIAL is for less sensitive information, but may include Personally Identifiable Information (PII) intended for use within an organization or by individuals, yet still requires a high level of security.

Examples: Accounting data, payroll data, sensitive customer information (taxation information)

INTERNAL USE ONLY (default category) is for non-sensitive information intended for use within your organization. The security is controlled, but not highly protected. This default category is to be used in the absence of any classification. This is the most prevalent category.

Examples: Procedures, operational work routines, project plans, designs and specifications, internal memos (usually; may also be classified as confidential at times), minutes of meetings, internal project reports.

UNCLASSIFIED/ PUBLIC is for information that requires minimal security and can be handled in the public domain.

Examples: Press statements approved for public use

Reclassification

Reclassification of information is ongoing as a regular part of maintaining your ISS program. The periodic review of classifications in conjunction with risk assessment will lead to appropriate protection and safeguard expenditure, rather than unnecessary expense.

Reclassification must be carried out with the approval of the security agency

Annexure A: Security Policy Guidelines

3.4.3 Asset Classification Summary

Classification Level	Impact	Storage	Tracking/ Disposal	Labeling	Release to Third Parties/Granting Access	Copying/ Faxing / E-mail
HIGHLY RESTRICTED	High Impact. Loss or damage WILL seriously impede the organizations future. Public or internal disclosure will cause critical harm to on-going operations or National Security.	Encrypted; physical access tightly controlled.	Track all recipients, copies made, locations sent, addresses, disposal method. Disposal - Shredding	Media – External and internal labels. Hard copy – each page should be labeled. Mail – address of specific person. No label on outside, only inside.	Owner approval and Non-Disclosure Agreement Highly restricted access or Owner only.	Distribution must be protected at all times. Owner approval for copying, faxing.
CONFIDENTIAL	Considerable Impact. Loss or damage COULD seriously impede the organization's future. Public or internal disclosure could cause harm to on-going operations or adversely impact National Security.	Encrypted; Physical Access controlled.	Tracking not required. Disposal – Shredding	Media – External and internal labels. Hard copy – each page should be labeled. Mail – address of specific person. No label on outside, only inside.	Owner approval and Non-Disclosure Agreement Highly restricted access or Owner only.	Distribution must be protected at all times. Owner approval for copying, faxing.

Annexure A: Security Policy Guidelines

Classification Level	Impact	Storage	Tracking/ Disposal	Labeling	Release to Third Parties/Granting Access	Copying/ Faxing / E-mail
INTERNAL USE ONLY	Minor impact. Loss or damage could cause minor concerns to the organization’s future. Public or internal disclosure could cause little or no harm to on-going operations.	Encryption Optional	Tracking not required. Disposal – no special process required.	No label required.	Non-Disclosure Agreement Local users only	No restrictions.
UNCLASSIFIED/ PUBLIC	No impact.	Encryption not necessary	Tracking not required. Disposal – no special process required.	Release Date	No restrictions	No restrictions.

Annexure A : Security Policy Guidelines

3.5 Risk Analysis

After you have given your assets a value, you can then measure the risks.

3.5.1 Calculating the Loss Impact

Taking a qualitative approach to evaluating your assets is very effective in grouping assets and applying ranges of impact losses. This saves a lot time and energy and is just as effective as getting to the exact dollars or Francs. The loss impact can be based on the replacement value, the immediate impact of the loss, and the consequence.

Loss Impact Calculations

Loss Impact (software) = Loss of Integrity cost+ Unavailability cost + Disclosure cost

Loss Impact (hardware) = Replacement cost + Unavailability cost

Where

Integrity Cost

Integrity measures the amount (cost) of damage that could be caused to the accuracy and completeness of the information and processing methods.

Scale (Cost)	Integrity Range (\$ or equivalent in Fr)
100	> \$1,000,000
75	\$500,000 – 1,000,000
50	\$100,000 - 500,000
25	\$25,000 – 100,000
10	\$1,000 - 10,000
1	< \$100

Unavailability Scale

The cost of unavailability involves both time and money. The inability to access information quickly can be devastating to many organizations e.g. the Army or in event of an epidemic. It depends on timing, duration, and the situation. Protecting against unavailability requires a high level of redundancy to eliminate possible points of failure protect not only the information, but also protect the access to it.

Scale (Cost)	Unavailability Range (\$ or equivalent in Fr)
100	> \$1,000,000
75	\$500,000 – 1,000,000
50	\$100,000 - 500,000
25	\$25,000 – 100,000
10	\$1,000 – 10,000
1	< \$100

Annexure A: Security Policy Guidelines

Disclosure Scale

Disclosure can be measured by its adverse effect of the agency or security.

Scale	Disclosure Impact
100	National Security impacted
50	Investment climate in the country affected
25	Adverse national press
10	Disclosure spread throughout the organization
5	Disclosure spread to another work area in your organization
1	Disclosure restricted to within the project or work area

\$ Cost to Replace Scale

The \$ cost to replace is the cost of recreation or replacement for hardware and communications devices only. It is the cost of purchasing, building, or having a service provide the replacement of the asset. It is both time and dollars.

If the cost of recreation is high, it must be given high rated safeguards, like redundant storage of asset, backup and recovery. It is usually easy to calculate given the fixed price of equipment at a given point of time and knowledge of implementation and customization costs.

Scale (Cost)	\$ Cost to replace (\$ or equivalent in Fr)
100	> \$1,000,000
75	\$500,000 – 1,000,000
50	\$100,000 - 500,000
25	\$25,000 – 100,000
10	\$1,000 – 10,000
1	< \$100

3.5.2 Calculating the Value

The value of an asset can be represented in terms of the potential loss and its effect on the business and its users. This value is used later in the asset risk factor calculation.

Value Calculation

Value = Storage + Users + Classification + Loss Impact

As calculated above

Annexure A: Security Policy Guidelines

3.5.3 Threats and Risks to Assets

Asset Threats

A threat is any circumstance or event with the potential to cause harm. Threats are always present. As the world's dependence on information continues to increase, threats become more worldwide, more ambitious, and increasingly more sophisticated. Before deciding how to protect a system, it is necessary to know what the system is to be protected against and what threats need to be countered.

A threat assessment is a critical part of the business impact analysis. The most important reason for identifying your threats is to know from what do the assets need protection and what is the likelihood that a threat will occur. Threats cannot be eliminated, but can be anticipated, and safeguards put in place to minimize their impact. **A threat is not an incident. With a threat, no event occurred, nothing has happened.**

Threat Types

Threats can be deliberate or non-deliberate, internal or external. The following table can be updated to reflect all threats and new attacks that could potentially occur.

Threat/ Risk Types	
Hackers	Virus, worm
Social Engineering	Trojan Horse
Competitors	Time bombs, stealth bombs, logic bombs
Insiders – authorized	Stealing information
Insiders - unauthorized	Disclosure
Former Employees	Defacement/ destroy and ruin
Script Kiddies	Change environment
Cyber-crime / Techno-crime	Denial of Service attack
Natural Disasters	Human error
	System failures
Add more	

Threat Likelihood

One of the main components in calculating asset risk factors is to determine the likelihood of a threat occurring to that asset. Estimating the chance that the threat will cause a loss is the main purpose. As specific threats are identified and assigned to each asset, a likelihood measure needs to be associated with the threat / asset pair.

Scale	Threat Likelihood
100	High likelihood
50	Moderate likelihood
1	Low likelihood

Annexure A: Security Policy Guidelines

Threat Impact

Impacts describe the effect of a threat on an asset. What are the immediate damages of the threat being realized? Impacts can be very specific (For example: change accounting data, falsify money transfers). The impact the threat could cause to that asset can be measured using the following scale:

Scale	Threat Impact
100	High impact. The effect is catastrophic; will cause National Security to be compromised or a large project to fail.
50	Medium to high impact. Significant loss to operations or citizen confidence. The effect is disastrous, but the organization can survive, at a significant loss.
25	Medium impact. Business operations are unavailable for a certain amount of time, revenue is lost, citizen confidence is affected minimally
10	Low to medium impact. Effect is minor, major business operations would not be affected.
1	Low impact. Impact is negligible.

Asset Risk Factor

A risk factor is required to understand the potential impact on information assets and to justify the expenditures on security safeguards. This risk analysis is a basic business process that should be performed on all major projects and new technologies before they are implemented to assure the feasibility of the projects. Since information systems technology is continually changing, risk analysis should be done periodically.

Security safeguards reduce risks. Although risks can be minimized, that cannot be eliminated. Security often focuses on worst cases scenarios, but typical scenarios are to also be considered. The "once in a million" scenario must be considered, but financial reasons may only implement the typical scenario.

Calculating the Risk Factor

The risk factor can be considered the representation of the kinds of adverse actions that may happen to information, the degree of likelihood that these actions may occur and the value of the asset. The outcome of this process should indicate the degree of risk associated with the defined value of the assets. This outcome is important because it is the basis for making safeguard selection and risk mitigation decisions.

Annexure A: Security Policy Guidelines

Risk Factor Calculation

Risk Factor = Value + Threat Likelihood + Threat Impact

The total possible points for the risk factor using the scales outlined above are 8 – 800 possible points where 8 is no risk and 800 is a disastrous level of risk.

The levels of high, moderate, low can be normalized and used to compare risks associated with each threat. You can change the scales and adjust the acceptable risk rating as your needs change.

Sometimes a risk factor that was derived from a high loss and low likelihood results in the same risk factor as one that resulted from a low loss and high likelihood. In these cases, you need to decide if the risk factor derived from the high loss is more critical than the risk factor derived from the high likelihood.

Acceptable Risk Rating

All assets will have some risk attached to them. You must decide on the acceptable risk rating for your organization. An acceptable risk rating would probably be something of the order of 200 in the above scale. This is a parameter for the security team to decide

Acceptable Risk Rating = 8 - _____

3.5.4 Safeguards and Assets

The most important and final step in the business impact analysis process is to determine what kind of protection or safeguards to implement. High-risk assets can then be re-evaluated and risk levels brought down to acceptable levels with prudent use of safeguards. Safeguards may also be called security measures, protective means, or counter measures.

All assets do not have the same potential of loss and do not require the same expenditure of protection. It is important to place the proper safeguard(s) on an asset that justifies the cost and maintenance. Threats cannot be eliminated, but can be anticipated, and safeguards put in place to minimize their impact.

Safeguards Types

Safeguard Types
Firewalls
VPN
Incident Monitors
Install all Patches
Intrusion Detection systems
Policies/ Rules/ Procedures
Awareness/ training
Logs - daily monitoring
Physical access means
Encryption/ disguise information
Mechanisms - password generator, token based, biometrics.
Software that will trace the source of attacks.

Annexure A: Security Policy Guidelines

Safeguard Types
Block all .exe files coming in from the outside
Backup and recovery
Redundant storage of asset
New hardware
Reporting
Password protection
Anti-virus / anti-spyware / anti-Adware software
Add Others

Assigning Safeguards

Safeguards should be assigned based on knowledge of the threats, the loss impact and the likelihood of its occurrence. Select those effective safeguards that will reduce the risk of an asset to an acceptable level. Safeguards can be used in combination and is a subjective process.

Recalculate the Risk Factor

After applying the proposed safeguard(s) to the asset, you must recalculate the risk factor for that asset. Is the remaining risk acceptable? The greater the risk factor, the more important it is to implement better safeguards.

Risk acceptance is described as an activity that compares the current risk factor with acceptance criteria and results in a determination of whether the current risk factor is acceptable. While effective safeguards and cost considerations are important factors, there may be other factors to consider such as: organizational policy, legislation and regulation, safety and reliability requirements, performance requirements, and technical requirements.

Assume the Residual Risk

After all safeguards are determined and the results of the new risk factor have been examined, the risk factor associated with the threat/ asset relationship should now be reduced to an acceptable level or eliminated.

Each organization needs to decide the amount of residual risk that it will be willing to accept after the selected safeguards are implemented. These initial risk acceptance decisions must be carefully considered. There may be risks that are determined to be too high, however, after reviewing the available safeguards, it maybe realized that the currently offered solutions are very costly and cannot be easily implemented into the current environment. This may force the organization into either expending the resources to reduce the risk, or deciding through risk acceptance that the risk will have to be accepted because it is currently too costly to mitigate.

The methodology defines safeguards in terms of security services and mechanisms. A security service is the sum of mechanisms, procedures, etc., that are implemented to provide protection.

The measures taken to protect assets should correspond to the value of the assets.

Annexure A: Security Policy Guidelines

Safeguard Costs

When considering the cost measure of the mechanism, it is important that the cost of the safeguard be related to the risk factor to determine if the safeguard will be cost effective. The cost of the safeguard is the amount needed to purchase or develop and implement each of its mechanisms. To calculate risk/ cost relationships use the risk factor and the cost associated with each safeguard and create a ratio of the risk to the cost. A ratio that is less than the cost of the mechanism is greater than the risk associated with the threat. This is generally not an acceptable situation (and may be hard to justify) but should not be automatically dismissed. Consider that the risk value is a function of both the loss measure and the likelihood measure. One or both of these may represent something so critical about the asset that the costly mechanism is justified.

Implementing and Testing Safeguards

The implementation and testing of safeguards should be done in a structured manner. The goal of this process is to ensure that the safeguards are implemented correctly, are compatible with other safeguards, and provide expected protection.

This process begins by developing a plan to implement the safeguards. This plan should consider factors such as available funding, and user learning curve. It should be recognized that not only is it important that the safeguard perform functionally as expected and provide the expected protections, but that the safeguard does not contribute to the risk through a conflict with another safeguard / functionality.

Each safeguard should first be tested independently of other safeguards to ensure that it provides the expected protection. This may not be relevant to do if the safeguard is designed to work with other safeguards. After testing the safeguard independently, the safeguard should be tested with other safeguards to ensure that it does not disrupt the normal functioning of those existing safeguards. The implementation plan should account for all these tests and should reflect any problems or special conditions as a result of the testing.

Annexure A: Security Policy Guidelines

3.6 How to do a Business Impact Analysis

3.6.1 How to identify information assets:

- Using the table given below, choose your information assets types: platforms, applications, general software, hardware and communications
- Update platforms in the Platform Table. Here you can list all applications or general software to safeguard them at the platform level and then you do not need to list them in the Applications table.
- Update applications in the Applications Table. You do not need to list those that are accounted for at the platform level. Example: payroll, drivers license, e-mail (Lotus Notes)
- Update general software in the General Software Table. Example: utilities, compilers, operating systems, user tools (MS Word)
- List hardware in the Hardware Table.
- List communications devices and entry points in the Communications Table.

For all asset types,

- Assign a physical or logical location (optional)
- Assign an inventory number (optional)

For all asset types (except communications):

- Using the table A, enter your ranges for the amount of storage/ disk space. Using this range, enter the scale for each asset in Table 2
- Using Table A, enter your ranges for the number of users. Using this range, enter the scale for each asset in Table B. This is the number of users that rely upon that asset.

For asset types - platform, applications, and general software:

- Enter the owner of the asset.
- Enter the classification scale for that asset

3.6.2 How to determine loss impact of an asset

For asset types - platforms, applications, general software:

Using Table A, enter your ranges for cost into the Integrity Scale Table. Using this range, enter the scale for each asset in Table B

Enter your ranges for cost into the Disclosure Scale Table. Using this range, enter the scale for each asset in Table B

For all asset types:

Enter your ranges for cost into the Unavailability Scale Table. Using this range, enter the scale for each asset in Table B

For asset types - hardware, communications:

Enter your ranges for the cost into the Cost \$ to Replace Scale Table. Using this range, enter the scale for each asset in Table B.

Annexure A: Security Policy Guidelines

3.6.3 How to calculate the value of an asset

For asset types - platforms, applications, general software:

Calculate the value = Storage + # Users + Classification + Loss Impact. This value is used later to calculate the asset risk factor.

For asset types - hardware, communications:

Value = Storage + # Users + Loss Impact. This value is used later to calculate the asset risk factor.

Annexure A : Security Policy Guidelines

Table A: Business Impact Analysis Ranges and Scales

Size in MB	Storage Classification - grade 1:100
25000+	100
10000+	80
5000+	60
2500+	40
1000+	20
< 1000	10

Number of Users	Usage Classification - grade 1:100
100+	100
75+	80
50+	50
25+	25
10+	20
< 10	10

Scale (Cost)	Integrity Range (\$ or equivalent in Fr)
100	> \$1,000,000
75	\$500,000 – 1,000,000
50	\$100,000 - 500,000
25	\$25000 – 100,000
10	\$1000 – 10000
1	< \$100

Annexure A: Security Policy Guidelines

Scale (Cost)	Unavailability Range (\$ or equivalent in Fr)
100	> \$1,000,000
75	\$500,000 – 1,000,000
50	\$100,000 - 500,000
25	\$25,000 – 100,000
10	\$1,000 – 10,000
1	< \$100

Security Level	Classification - grade 1:100
Highly restricted	100
Confidential	80
Internal use only	50
Unclassified / Public domain	1

Scale	Disclosure Impact
100	National Security impacted
50	Investment climate in the country affected
25	Adverse national press
10	Disclosure spread throughout the organization
5	Disclosure spread to another work area in your organization
1	Disclosure restricted to within the project or work area

Scale (Cost)	\$ Cost to replace (\$ or equivalent in Fr)
100	> \$1,000,000
75	\$500,000 – 1,000,000
50	\$100,000 - 500,000
25	\$25,000 – 100,000
10	\$1,000 – 10,000
1	< \$100

Annexure A: Security Policy Guidelines

Scale	Threat Likelihood
100	High likelihood
50	Moderate likelihood
1	Low likelihood

Scale	Threat Impact
100	High impact. The effect is catastrophic; will cause National Security to be compromised or a large project to fail.
50	Medium to high impact. Significant loss to operations or citizen confidence. The effect is disastrous, but the organization can survive, at a significant loss.
25	Medium impact. Business operations are unavailable for a certain amount of time, revenue is lost, citizen confidence is affected minimally
10	Low to medium impact. Effect is minor, major business operations would not be affected.
1	Low impact. Impact is negligible.

Annexure A: Security Policy Guidelines

Table B: Business Impact Analysis — Platform Table

ISS Asset: Platform (option: list all categories)	Location (physical or logical platform/ location)	Inventory Number (number)	Storage space/ size (scale)	#Users: usage and sharing (scale)	Owner (name)	Classification (scale)	Loss Impact			Value (Storage + Users + Class + Loss Impact)
							Integrity (scale)	Unavail-ability (scale)	Disclosure (scale)	

ISS Asset: Platform (option: list all categories)	Threat (list all)	Threat Likelihood (scale)	Threat Impact (scale)	Risk Factor (Value + Threat Likelihood + Threat Impact)	Current Safeguard(s) (list)	Proposed Safeguards		
						(list)	New Risk Factor (Value + Threat Likelihood + Threat Impact)	Costs (\$/RwFr)

Annexure A: Security Policy Guidelines

Table B: Business Impact Analysis — Applications Table

ISS Asset: Platform (option: list all categories)	Location (physical or logical platform/ location)	Inventory Number (number)	Storage space/ size (scale)	#Users: usage and sharing (scale)	Owner (name)	Classification (scale)	Loss Impact			Value (Storage + Users + Class + Loss Impact)
							Integrity (scale)	Unavail- ability (scale)	Disclosure (scale)	

ISS Asset: Platform (option: list all categories)	Threat (list all)	Threat Likelihood (scale)	Threat Impact (scale)	Risk Factor (Value + Threat Likelihood + Threat Impact)	Current Safeguard(s) (list)	Proposed Safeguards		
						(list)	New Risk Factor (Value + Threat Likelihood + Threat Impact)	Costs (\$/RowFr)

Annexure A: Security Policy Guidelines

Table B: Business Impact Analysis — General Software Table

ISS Asset: Platform (option: list all categories)	Location (physical or logical platform/ location)	Inventory Number (number)	Storage space/ size (scale)	#Users: usage and sharing (scale)	Owner (name)	Classification (scale)	Loss Impact			Value (Storage + Users + Class + Loss Impact)
							Integrity (scale)	Unavail-ability (scale)	Disclosure (scale)	
Operating Systems										
Utilities										

ISS Asset: Platform (option: list all categories)	Threat (list all)	Threat Likelihood (scale)	Threat Impact (scale)	Risk Factor (Value + Threat Likelihood + Threat Impact)	Current Safeguard(s) (list)	Proposed Safeguards		
						(list)	New Risk Factor (Value + Threat Likelihood + Threat Impact)	Costs (\$/RwFr)
Operating Systems								
Utilities								

Annexure A: Security Policy Guidelines

Table B: Business Impact Analysis — Hardware Table

ISS Asset: Hardware	Location (physical or logical location)	Inventory Number (number)	Storage space/size (use scale)	#Users – usage and sharing (use scale)	Loss Impact		Value (Storage + Users + Loss Impact)
					\$ to Replace (use scale)	Unavailability (use scale)	
Processors							
Printers							
UPS							

ISS Asset: Hardware	Threat (list all)	Threat Likelihood (scale)	Threat Impact (scale)	Risk Factor (Value + Threat Likelihood + Threat Impact)	Current Safeguard(s) (list)	Proposed Safeguards		
						(list)	New Risk Factor (Value + Threat Likelihood + Threat Impact)	Costs (\$)
Processors								
Printers								
UPS								

Annexure A: Security Policy Guidelines

Table B: Business Impact Analysis — Communications Table

ISS Asset: Communications	Location (physical or logical location)	Inventory Number (number)	Loss Impact		Value (Storage + Users + Loss Impact)
			\$ to Replace (use scale)	Unavailability (use scale)	
Access points/ configuration points					
Modems					
Routers (list quantity by model)					
Networks					
Switches					

ISS Asset: Communications	Threat (list all)	Threat Likelihood (scale)	Threat Impact (use scale)	Risk Factor (Value + Threat Likelihood + Threat Impact)	Current Safeguard(s) (list)	Proposed Safeguards		
						(list)	New Risk Factor (Value + Threat Likelihood + Threat Impact)	Costs (\$/RwFr)
Access points/ configuration points								
Modems								
Routers (list quantity by model)								
Networks								
Switches								

Annexure A : Security Policy Guidelines

3.6.4 How to identify threats/ risks to assets

- Update the Threats/ Risk Types table with your organizations threat/ risk types in Table C.
- Using Table B, assign a threat type to each asset.
- Assign the threat likelihood that it will occur to that asset.
- Assign the threat impact it will have on that asset.
- Calculate the Risk Factor for each asset.
- Determine the Acceptable Risk Factor for your organization.

3.6.5 How to safeguard your assets

- Update the Safeguards Table in Table D with both current and proposed safeguards.
- Enter current safeguard(s) for each asset from the list in the Safeguards table.
- Enter proposed safeguard(s) for each asset from the list in the Safeguards table.
- Recalculate the Risk Factor by reevaluating asset.
- Enter the safeguard cost. Select cost effective safeguard.
- Accept Residual Risk

Annexure A: Security Policy Guidelines

Table C: Threats/Risks Types Table

Threat/ Risk Types	
Hackers	Virus, worm
Social Engineering	Trojan Horse
Competitors	Time bombs, stealth bombs, logic bombs
Insiders – authorized	Stealing information
Insiders - unauthorized	Disclosure
Former Employees	Defacement/ destroy and ruin
Script Kiddies	Change environment
Cyber-crime / Techno-crime	Denial of Service attack
Natural Disasters	Human error
	System failures
Add more	

Scale	Threat Likelihood
100	High likelihood
50	Moderate likelihood
1	Low likelihood

Scale	Threat Impact
100	High impact. The effect is catastrophic; will cause National Security to be compromised or a large project to fail.
50	Medium to high impact. Significant loss to operations or citizen confidence. The effect is disastrous, but the organization can survive, at a significant loss.
25	Medium impact. Business operations are unavailable for a certain amount of time, revenue is lost, citizen confidence is affected minimally
10	Low to medium impact. Effect is minor, major business operations would not be affected.
1	Low impact. Impact is negligible.

Annexure A: Security Policy Guidelines

Safeguard Types
Firewalls
VPN
Incident Monitors
Install all Patches
Intrusion Detection systems
Policies/ Rules/ Procedures
Awareness/ training
Logs - daily monitoring
Physical access means
Encryption/ disguise information
Mechanisms - password generator, token based, biometrics.
Software that will trace the source of attacks.
Block all .exe files coming in from the outside
Backup and recovery
Redundant storage of asset
New hardware
Reporting
Password protection
Anti-virus / anti-spyware / anti-Adware software
Add Others

_____ Acceptable Risk Rating

Annexure A: Security Policy Guidelines

Table D: Safeguards Table

Safeguard Types	What it Protects	Rating
Firewalls.		
VPNs		
Incident monitors.		
Install all patches.		
Intrusion detection systems.		
Policies/rules/procedures.		
Awareness/training.		
Logs - daily monitoring.		
Physical access means.		
Encryption.		
Mechanisms - password generator, token-based, biometrics.		
Software that will trace the source of attacks.		
Block all .exe files coming in from the outside.		
Backup and recovery.		
Redundant storage of asset.		
Anti Virus		
Anti Spam / Adware		
Add more ...		

4 Security Management Team

Responsibility for information security is everyone's duty as it affects every department and every person in an organization. Information appears everywhere in an organization, and almost every worker uses information to do their job.

In addition to having aware employees, it is also necessary to have a security team that concentrates on protecting and monitoring systems. There may be several security teams:

- Security day-to-day
- Security advisory committee(s)
- Security incident response team
- Government Security Agency

Security Day-to-Day

Protecting and monitoring information security is a daily task. There are security administration tasks that involve new authorizations and access controls. Security monitoring involves checking logs and intrusion reporting systems, and reviewing plans and procedures as needed.

Checking critical reports and system usage is one of the most important daily tasks. A good set of procedures should be put in place to effectively manage the security function(s).

Security Advisory Committee(s)

Most large agencies should assemble a Security Advisory Committee. This advisory group / steering committee should be made up of key technical and management personnel within the organization to coordinate security efforts and resolve security problems with overall authority over all aspects of security. The security officer coordinates this effort.

Each organization should also select a member for the incident response, or Computer Emergency Response Team (CERT). This CERT team provides assistance and gets involved with your organization in the event of an incident.

Incident Response Team

Each organization should assemble an Incident Response Team to handle all suspicions and incidents. This team may be some of the Security Advisory Committee members.

It is critical that someone on the incident response team be designated to produce the documentation that describes the events and outcomes.

Annexure A: Security Policy Guidelines

The Government Security Agency

A pan-government agency is required that implements the Security Policy, maintains the guidelines and Policy, advises agencies on security matters and conducts periodic audits to ensure compliance. A senior security expert from a key ministry or agency should head this agency (e.g. Ministry of Defence or the Army). This agency will have the ultimate responsibility for maintaining Information security in the country.

The Security Officer

One of the key appointments in any organization is to designate a Security Officer. In smaller organizations, the ISS Officer may not be a full-time security specialist, but may also have other technical or business related job functions. In the larger agencies, the ISS Officer may perform ISS tasks full time and may even require additional security staff to accomplish all security tasks. In both situations, someone needs to be appointed to take the overall responsibility of ensuring that the appropriate ISS safeguards are in place, the policies and procedures are agreed and rolled-out, and that all users of information understand their responsibilities and duties. Usually ICT administrators within the line ministries will also have the responsibility for managing Security.

The Security Officer is responsible for overseeing the entire security process. The primary role is to ensure each organization's information is protected.

Security officer are expected to perform the following tasks:

Rule Tasks
Recommend, develop and set up security rules
Implement enterprise, organization-specific and application-specific security rules and procedures
Enforce ISS rules
Monitor compliance to security rules
Periodically evaluate effectiveness of ISS rules and procedures
Gather facts and analyze information security issues/ keep current
Develop recommendations for the agency on ISS matters
Systems Tasks
Act as liaison between security department and IS
Coordinate follow up procedures for ensuring proper adjustment of access privileges associated with changes in employee status and business arrangements.
Develop procedures and administer the information access control decisions made by information custodians within the organization.
Review changes to the configuration of security administration facilities and settings
Participate in preparing a disaster recovery plan to help prepare contingencies and be ready to implement the disaster recovery plan
Implement procedures for authentication of users and messages
Publish guidelines for creating and managing passwords
Approve/ disapprove access by users to systems/ set up access (passwords)
Cooperate in the development and implementation of security technology
Perform security assurance reviews for new systems and changes to existing systems
Maintain up-to-date records for all systems accessed by employees and users
Maintain configuration profiles of all systems controlled by IS including but not limited to mainframes, distributed systems, microcomputers, and dial access ports.
Identify security technical resources and tools
Document the security support structure across platforms.
Participate in reviews and analysis of internal projects that may have impact on ISS.

Annexure A: Security Policy Guidelines

Security Tasks
Investigate, coordinate, report, and follow-up on security incidents
Coordinate prosecution of offenders
Assign an owner to each asset
Provide interface with internal and external audit agencies
Conduct business impact analysis - risk assessments to identify threats and potential safeguards
Assemble a security team
Monitor unusual activities and report security breaches and incidents, including identifying resources to assist with tracking, analysis, and responding to incidents.
Establish and chair agency security committees.
Report risks and incidents to agency head - all areas
Furnish security awareness, training, and advisory programs for employees
Establish and maintain security teams with roles and responsibilities
Identify training requirements
Develop and implement strategies to make users aware of security rules, procedures, and benefits.
Coordinate technical leads and public relations
Establish secure communication channels/ conduct regular training and readiness drills
Monitor, audit, and test systems for security vulnerabilities.

Security Officer Training

The Government Security Agency will be responsible for training the security staff including the security officers. Periodic training courses and refresher regimes should be carried out to enable the security apparatus to meet new and ubiquitous threats.

Conferences are held throughout the year in several parts of the world. The following are recommended:

CERT
InfoSecurity
IBM Global Services
RSA

Certifications can be received in:

CISSP
CISA

Security Staff

The security officer may perform ISS tasks full time and still may even require additional security staff to accomplish all security tasks. This will be true only for large organizations such as the Army or Ministry of Finance / Defense

The security officer and the IS department work very closely together, especially the systems and network administrators who set up accesses and track usage. It is critical that the security officer have full cooperation from the IS department. Systems programmers, computer operators, managers, and IS clerical staff may also be critical to the security process.

Annexure A: Security Policy Guidelines

Security Guards

Not all organizations will have the need for a guarded entry to a building or room. If they do, physical access becomes the responsibility of the security guards. Many companies support the physical entry process by providing equipment, software, tools, and even the guards.

Copyright Contact

Each employee must comply with copyright laws. Organizations should communicate this to all employees and should designate a single point of contact for inquiries about copyright violations, pursuant to the law.

Security Auditors

Large organizations must have their own internal security auditor(s) who track daily traffic. The Security Agency must assist in this role and carry out assessments for smaller organizations that are considered at risk. All developed applications must include auditing capabilities to track access to sensitive information.

Some standard guidelines for conducting audits are given below. These are not exhaustive or comprehensive and not meant to represent an Audit manual.

Security Audits

A security audit is performed to keep security tight and anticipate weak areas. An audit can also be thought of as an assessment or vulnerability test to review existing practices. Day-to-day tracking and monitoring of logs and reports can also be thought of as an audit function. Therefore audits can be:

- Daily tracking and monitoring
- Formal Audit (assessment)
- Surveillance audits (re-assessments)

In a formal audit, an independent, third party auditor is required to regularly audit the security program. It is recommended that this is performed every 6 months, or at least once a year. The security agency can be entrusted the role of carrying out the audits if the staff is available.

Annexure A: Security Policy Guidelines

What should be audited?

- All new systems installations to ensure conformance to existing policy statements.
- Perform regular automated system checks to reveal possible intruder activity or illicit behavior by insiders.
- Random security checks
- Audit critical files (i.e. passwords) to assess their integrity and look for unauthorized changes.
- Audit user account activity on a regular basis to detect dormant, inactive, or misused accounts anomalies.
- View logs (For example: # user attempts to log on)
- You can audit from the inside out (on-site), or from the outside in (off-site).
- Dormant User IDs for {} days
- User Log on Register or some type of operator / admin logs show incorrect or unusual entries, it could indicate that data has been accessed and therefore possibly lost or stolen.
- Applications must include auditing capabilities to track access to sensitive information.

Daily Audit/ Tracking Logs

Logs, or reports should be used to manage and monitor activity on your system. At least some of the following logs must be maintained:

- Logs Required On Application Systems Handling Sensitive Information
- Keystroke Logs Required For All Production System Privileged User-Ids
- Security Relevant Events In System Logs
- Computer System Logs Must Support Audits
- Accountability And Traceability For All Privileged System Command
- Contents Of Logs For Systems Running Production Applications
- Required Retention Period Of Logs
- Daily Removal Of Logs From Internet-Accessible Computers
- Logs Of User-Initiated Security Relevant Activities
- Retention Of Access Control Privilege Logs
- Information To Capture When Computer Crime Or Abuse Is Suspected
- Logs Required For Rapid Resumption Of Production System Activities
- Systems Architecture For Logging Activities
- Clock Synchronization For Accurate Logging Of Events On Network
- Logs Of All Inbound And Outbound Faxes
- Writing Logs To WORM Storage Media Prevents Alteration
- Persons Authorized To View Logs
- Regular And Prompt Review Of System Logs
- Notification Of Users About Logging Of Security Violations

Annexure A: Security Policy Guidelines

Suggested logs by User ID:

1. Log on attempts failed
2. Actions performed
3. High profile actions
4. Wide scale deletions
5. Who edited website
6. Activities of computer operations
7. Activities of system administrators
8. Activities of security officers
9. Who accessed highly sensitive data

Most logs should report time, date, User ID, type of event, success or failure, origin of request (i.e. terminal address), etc

Annexure A : Security Policy Guidelines

Summary of Security Officer Tasks

ISS Tasks	Agency/ Department (if different)	Division/Unit Responsible	Person(s) Responsible	Position
Recommend, develop, and implement security Rules				
Enforce and monitor compliance to security Rules.				
Periodically evaluate effectiveness of ISS Rules and procedures.				
Act as liaison between security department and IS.				
Coordinate follow up procedures for ensuring proper adjustment of access privileges associated with changes in employee status and business arrangements.				
Review changes to the configuration of security administration facilities and settings.				
Participate in preparing a disaster recovery plan to help prepare for contingencies and be ready to implement the disaster recovery plan.				
Implement procedures for authentication of users and messages.				
Publish guidelines for creating and managing passwords.				
Approve/disapprove access by users to systems/set up access – passwords.				
Cooperate in the development and implementation of security technology.				
Perform security assurance reviews for new systems and changes to existing systems.				
Maintain up-to-date records for all systems accessed by employees and users.				
Maintain configuration profiles of all systems controlled by IS				
Identify security technical resources and tools.				

Annexure A: Security Policy Guidelines

ISS Tasks	Agency/ Department (if different)	Division/Unit Responsible	Person(s) Responsible	Position
Document the security support structure across platforms.				
Participate in reviews and analysis of internal projects that may have impact on ISS.				
Gather facts and analyze information security issues/ keep current.				
Investigate, coordinate, report, and follow up on security incidents.				
Coordinate prosecution of offenders.				
Assign an owner to each asset.				
Provide interface with internal and external audit agencies.				
Conduct business impact analysis - risk assessments to identify threats and potential safeguards.				
Assemble a security team.				
Monitor unusual activities and report security breaches and incidents, including identifying resources to assist with tracking, analysis, and responding to incidents.				
Establish and chair agency security committees.				
Report risks and incidents to agency head - all areas.				
Furnish security awareness, training, and advisory programs for employees.				
Establish and maintain security teams with roles and responsibilities.				
Identify training requirements.				
Develop and implement strategies to make users aware of security Rules, procedures, and benefits.				
Coordinate technical leads and public relations.				
Establish secure communication channels.				
Conduct regular training and readiness drills.				

Annexure A: Security Policy Guidelines

ISS Tasks	Agency/ Department (if different)	Division/Unit Responsible	Person(s) Responsible	Position
Monitor, audit, and test systems for security vulnerabilities.				

5 Creating an Awareness Program

5.1 What is ISS Awareness?

Information Systems Security (ISS) awareness is an important part of any security plan or program. Employees at all levels need to understand that they play a large part in protecting their organizations information assets. Awareness teaches employees that they are a key piece of the total security environment. Through training and on-going reinforcement, everyone will begin to "Think Security" as a matter of daily practice. Only with full support and cooperation of all employees can a successful ISS program be established and maintained.

While training is sometimes one of the first items to feel the budget pinch, a good training program is usually more valuable than several audits, prevention mechanisms and safeguards put together. An awareness program process has two major parts:

- Awareness briefing (initial rollout)
- Continuous awareness materials

Awareness Briefings

All employees should be taught the importance of information security, what the rules are that must be followed, and what to do if there is a violation. An ISS awareness program is critical to any ISS program design. Increased awareness increases the proper use of security principles and the likelihood that suspicious activities will be noticed and reported.

Before granting access to systems, all employees should receive at least a Security Awareness information packet.

ISS policy and standards are ineffective if individuals at any level of the organization are unaware of the importance of security policy, do not understand established standards or fail to perform required practices for any reason. Good security is "a state of mind" that can best be achieved by a program or process that reinforces the concern and appropriate actions on a regular and ongoing basis.

Continuous Awareness Materials

Information Security is not a one-time event, nor is it a "volume of rules sitting on the shelf". Good security practices are not always obvious, intuitive or easily incorporated into established routines. To have maximized effectiveness information security standards must be known, understood, believed to have value, and appropriately and consistently practiced.

A program that offers continuous reinforcement of the organization's position with regard to handling the many aspects of ISS provides the tone and commitment to support greater sensitivity to the potential of an unwanted compromise or loss of assets.

Annexure A: Security Policy Guidelines

On-going and positive reinforcement for the necessity for information security policy and standards provides awareness and a “mind set” that encourages the intended practice of the established procedures. Without such reinforcement, policies or standards may be perceived as not relevant, necessary, or valuable and may be “followed” but not be practiced in a manner that supports full effectiveness.

The following are suggestions for ways to keep the awareness program alive:

- Refresher classes
- Regular updates to materials
- Top management communications to staff
- Conduct regular readiness drills
- Poster reminders

As technology and business needs change, the program will need to be revamped accordingly.

5.1.1 What is an Awareness Program?

An ISS awareness program brings ISS to a personal level. Everyone is responsible for the security of the information they use. The purpose of an awareness program is to teach the audience how to incorporate the rules and procedures into their daily operations.

Incorporating an Awareness Program

ISS awareness can be incorporated into the following workshops:

- Initial ISS program rollout
- Continuous awareness refresher courses
- New hire orientation

Security is Everyone’s Business

ISS is every worker's duty on a day-to-day basis. Specific responsibility for information security is NOT solely vested in the Information Security Department. Information security is multi-departmental, multi-disciplinary, and multi-organizational in nature. **This means that a single department within an organization cannot possibly adequately address information security.**

Every employee must do their part in order to achieve appropriate levels of information security. After all, information can be found nearly everywhere in the organization and nearly every employee utilizes information in order to do his or her job. It is only natural that every employee should be specifically charged with responsibility for information security.

Annexure A: Security Policy Guidelines

Awareness Applies to Everyone

All employees (employees, consultants, contractors, temporaries, etc.) are required to receive the same level of ISS awareness and training. This training requirement should be included as appropriate in all contracts. Workers must be provided with sufficient training and supporting reference materials to allow them to properly protect your organization's information resources. Management must allocate sufficient on-the-job time for employees to acquaint themselves with the organization's security rules, procedures, and related ways of doing business.

Security and Performance Reviews

Some organizations may want to go one step further and incorporate a question into performance review forms. The question could read something like this: "Does the employee observe information security policies in the course of his/her work?"

This must be supplemented with additional instructions, telling employees exactly what is expected of them.

Mandatory Awareness Training

ISS training should be mandatory. Every employee must attend an information security awareness class soon after the date of employment. To provide evidence that every employee has attended such a class, each employee must sign a statement that they have attended a class, understood the material presented, and had an opportunity to ask questions.

Signed Agreements

Without confirmation that all new and existing employees are aware of security policy there is no assurance that the desired actions are understood or followed. Failure to follow policy or practice standards for any reason reduces the value of such statements to "documents of prosecution" and negates the positive reinforcement and protective intent for which the information policy and standards exist.

Many organizations abroad require users to sign a statement that they agree to:

- abide by information security policies and procedures. A signature on a form with this statement, and perhaps a summary of the policies and procedures, can be required before a user is given a user-ID and a password.
- their understanding of the code of conduct by annually signing a form acknowledging that they agree to subscribe to the code. The intention is to annually remind employees that they must abide by the organization's code of conduct. From a legal standpoint, it is desirable to have employees acknowledge in writing that they have read and understand that a code of conduct is a required part of their job. If they are subsequently terminated due to code of conduct related problems, there is no doubt that the employee understood what was required of him or her. This agreement therefore reduces the probability of a wrongful termination lawsuit.
- to provide evidence that every employee has attended ISS class, each employee must sign a statement that they have attended a class, understood the material presented, and had an opportunity to ask questions. For existing employees, a modification of this agreement could state they must attend within **{6}** months of the date when such courses become available.

Annexure A: Security Policy Guidelines

Every worker must understand the ISS rules and procedures and must agree in writing to perform his or her work according to such rules and procedures.

All employees with access to computer systems must be informed of security policies and procedures and their responsibilities in writing. All new employees with access to critical systems or sensitive information will sign a statement acknowledging they have received and read the policy and understand their responsibilities. This should include knowledge of the consequences of violations of security procedures.

A signed statement indicating awareness, compliance and intent of continued compliance with information security policy and standards will be required upon annual review of each employee with access to critical systems or sensitive information.

Contractors, agents acting on behalf of the agency, auditors, and other non-employees in a position to impact the security or integrity of information assets of the state will be made aware of the Information Security Policy. These individuals must sign a statement acknowledging they have received and read the policy and understand their responsibilities.

Annexure A: Security Policy Guidelines

5.1.2 What makes up an Awareness Program

An awareness program can be delivered in many ways. Initially, when the ISS program is rolled out awareness training in a classroom environment is the best option. A classroom environment with a standardized curriculum gives a consistent message to all attendees and encourages interaction and discussion.

An awareness program can consist of the following:

- Campaign
- Materials
- Training

Awareness Campaign

An awareness campaign is a good way to initially incorporate the ISS program. A campaign can “advertise” that the ISS program is coming soon and with good promotional items, you can gain employee’s attention, emphasize key points, and even educate them on key security issues.

Campaign Mottoes/ Themes

You may want to start a theme that identifies the ISS program or the awareness program itself. For example: call the training class “Security 101”, or “Think Security”.

The T.E.A.M. approach (Together Everyone Achieves More) is also effective to bring everyone together as one complete ISS program having the concept that we will have to all work together to make it a success.

Campaign Ideas

- Stage vulnerability demonstrations
- Give small prizes (i.e. free lunch) for exemplary staff (i.e. reported a violation)
- Give “traffic ticket” warnings reflecting rule violations. (i.e. workstations not logged out or locked during a fire drill)
- Initiate an unannounced “unauthorized software duplication” inventory where PCs are checked for illegal software.
- Adopt an annual ISS day with special educational materials and events.
- Develop a “tagline” or theme that represents ISS at your organization

Annexure A: Security Policy Guidelines

5.1.3 Awareness Materials

The template package helps to prepare your ISS program materials. You may need to develop additional training materials, checklists, and such for your organization's particular needs.

Suggested awareness materials:

- Training Guides
- E-mail messages
- Articles in your organization's newsletter
- Magazines, Internet articles for circulation
- Bulletins and alerts
- Posters
- FAQs
- Web announcements
- Labels for system (PC), diskettes, etc
- Handouts
- Overhead slides
- Exercise workbook
- Quiz (to measure results)
- Practice sessions (do mock security drills)
- Presentation tool
- Class Evaluation
- Giveaways – buttons, pens, certificates, t-shirt's, mouse pads, ...

Awareness Training

The best way to educate your employees on ISS awareness is in a training classroom environment. The curriculum for the class can follow the same sequence as the guides you created from the templates.

Training Purpose

To teach the attendees how to recognize security issues, to be involved in the overall security of the organization, and to know what to do if they encounter an incident.

Training Logistics

- Self-teaching or classroom
- Informal, workshop, seminar
- Role playing
- Stage mock incidents to see responses
- On-the-job training
- Other Special Training Topics on case by case basis

Annexure A: Security Policy Guidelines

Training Audience

The training audiences can be very general or very specific to certain job tasks. The following lists the main audiences that require ISS awareness training.

Management

Management at any level may require a different view of ISS business practices. Upper level management may need simply an executive overview, while middle management and user department management may need to know more about prevention, detection, and incident reporting.

Although management is a separate audience, the materials and curriculum are a subset of the Computer User (permanent staff) course.

Computer User (permanent staff)

The largest of all audiences, the general computer user (permanent staff) audience requires a unique training class

Computer User (temporary staff)

The computer user (temporary staff) audience may not need as much training as the permanent staff since HR issues and such do not apply. They are not necessarily a separate audience, but are a subset of the computer user (permanent staff) class. They could also be combined/ incorporated with computer user (permanent staff).

Contractors, Agents, Auditors and non-Employees

See Computer User (temporary staff) above.

Technical Staff/ Management

This is a highly specialized and separate audience from the Permanent Staff group. They require a specialized training class

This audience will also take the computer user (permanent staff) class.

Security Officer/ Staff

The security department consisting of a security officer and security staff is a separate audience and they require specialized training classes in security audit, advanced topics, certification, etc.

Annexure A : Security Policy Guidelines

Awareness Program

Awareness Topics/ Curriculum	Audience	Purpose	Campaign	Training	Materials Needed

Computer User Awareness Training: Sample Agenda

Topics

Duration (min.)

Class Opening

Intros/Logistics/Class Overview	10
Project Overview	10
Management Support	10

Subjects

ISS Overview	30
Incident Reporting	15
Computer User Rules Overview	5
Access Control Rules	10
Network Security Rules	10
Internet, E-mail Rules	15
Workstation/Office Rules	5
Physical/People Rules	5
Copyright Rules	5
Acceptable Use Rules	10

Closing

Summary Test	10
Wrap Up/What's Expected	5
Final Q&A	3

Quiz

Total Duration:

158 min. (2 hr, 38 min.)

6 Incident programs

6.1 What is an Incident Program?

In your ISS plan, the most important program you can implement is one that handles suspicions and incidents quickly, investigates them thoroughly and takes prompt, corrective action if required. You need to be in position to react, detect, and resolve. **The key to a good response is having a team established, trained, and ready to react to any and all occurrences.** The IS department is the biggest part of the incident response team to provide the technical knowledge and evidence preservation but it may also comprise of line managers and others from different disciplines.

The three main components that make up the Incident Program are:

- Prevention
- Detection
- Response

Suspicious and Incidents

Security incidents or security breaches can occur at anytime. Prompt attention to reacting to reported incidents could greatly deter the amount of damage, loss, or disclosure that has taken place.

A suspicion, an unconfirmed assumption of attack, is not yet an incident. For this reason, it is even more critical to report a suspicion so as to avoid the incident from even happening or greatly decrease any negative results.

It is the responsibility of every employee to do their part in detecting and reporting any possible incidents or suspicions.

Prevention

Prevention is the key to good security practices, however, even with all the proper protection methods in place, there are always ways to compromise it. In order to know how to prevent incidents, you need to know what your assets are, where the risks lie, and how to protect critical information from being targeted.

Annexure A: Security Policy Guidelines

Detection

Detection is the only way of knowing when a system is being compromised. Without proper detection, it may never be known when an incident has occurred and therefore it may continue to happen. Even worse than having a security incident is having one and not knowing it.

To understand intrusion detection, one must be aware of the intruder, where attacks come from, what motivates them, how attacks occur, and who the attackers are. Not all organizations have the resources to conduct their own intrusion detection and analysis. In these situations, it may be necessary to identify other sources for assistance in tracking and responding to possible incidents.

Detection may be the difference between an incident and a disaster

Intrusion Detection Methods

There are many methods used to detect suspicious system behavior. Some methods will keep the intruder busy, while he is tracked down. Others will lock the intruder out until he is discovered.

It is important that detection methods not only find known attacks scenarios, but also new scenarios. Detection methods should look for the unusual and unexpected.

Intrusion detection systems (IDS) exist to help you safeguard your assets. These systems can monitor configurations, compare user actions, and distinguish conflicts in activities. IDS runs constantly with your system in the background and only notifies you when it detects something suspicious or illegal.

Tracking Intrusions

Your organization shall implement procedures for logging information on intrusion attempts and storing that information in a manner for later analysis or use by law enforcement.

Incident Patterns

It is important that all suspicions and incidents be logged and carefully tracked for patterns in behavior, timing, or other such tracking technique.

Response/ Reaction

Now that you have all your safeguards in place and are actively practicing good detection techniques, you can only hope that you have thought of everything. As many ways as there are to prevent mishap, there are just as many to circumvent your safeguards.

The key to further protecting your information even in the event of an attack is to have a good response plan implemented. A quick reaction can greatly diminish the damage.

If you do not have an incident response team established, you are depending on the reactions of users, IT and management to react, thus possibly turning a containable incident into a serious problem.

Annexure A: Security Policy Guidelines

Your Incident Response Team

The security team should be responsible for the reaction to an incident. Periodic mock drills are recommended for each possible type of attack.

Incidents Response Centers

There are companies that can assist in the incident handling process, but your internal response is the key. These companies can help you after the fact, with collecting and processing evidence and furthering the reporting to law enforcement and such if required.

Catastrophic Event

For catastrophic disasters such as fire, bomb threats, hostage situations, floods or destructive storms, the goals of employee safety and damage containment apply. Notification procedures will include the appropriate public service departments (Fire Department or Police Department).

Secured Area Intrusion

For intrusion of secured areas, the goals of employee safety, intruder identification, and intruder removal from the premises are applicable. Notification procedures will include building security or local police.

Virus Reporting

The greatest danger with a computer virus is that if it goes unreported and uncontained, it will continue to spread. Computer viruses can spread quickly and need to be eradicated as soon as possible to limit serious damage to computers and data. You must report a computer virus infestation immediately after it is noticed. Prevention is better than cure. Though there is no universal industry standard for Anti-virus software, several popular products perform equally well and are reasonably economic. Norton Anti-virus, McAfee Anti-virus, Panda anti-virus are popular packages. AVG from Grisoft is a popular free software available for Windows and Linux machines.

Electronic Intrusion

For cases involving electronic intrusion, the goals of data integrity, data recovery, method of breach and intruder identification apply. Notification procedures must include the Security Agency and may include the Police (if deemed serious enough), the potentially affected business area manager, software application support manager, and data center manager. Any activity monitor data, collected as a normal part of doing business, should be kept until the incident has been cleared.

All Intrusion detection systems must conform to the standards set by SNORT (www.snort.org). Black Ice is a standard product that provides several features for less than US\$ 40/- per desktop (bulk discounts and Server systems are also available). Any equivalent product can be used.

Unauthorized Access Intrusion

Whenever unauthorized system access is suspected or known to be occurring, you must take immediate action to terminate the access. If these actions do not completely suppress the unauthorized activity, assistance from the other designated contacts (i.e. security guard) must immediately be sought. It is every employee's responsibility to be aware of strangers or unidentified persons on the premises.

Annexure A: Security Policy Guidelines

Notifying the Intruder – yes or no?

In some cases, a stern cease and desist message must be sent to the source of all attacks against your organization's computers whenever the source or intermediate relay points can be identified. The intention of this is to send a message to attackers that their activities have been noticed and that they should stop immediately. Such a message may, in some instances, be enough to discourage an intruder from further efforts. If an attacker is using a shield such as a relay site, then the message can still be sent to the relay site's administrator. Even if the attacker doesn't get the cease and desist message, someone who manages that site can still take action, such as revoke the privileges of the offending User ID or otherwise tighten-up security.

Web Site - Contact Information

Sometimes someone outside your organization can be valuable in helping to detect an incident (e.g. a web page modified by hackers, and then noticed by a potential customer). In an indirect way, this solicits outsiders to assist with information security. Often customers and prospects are the first to notice there is a problem. The inclusion of contact information on web pages helps outsiders to report problems. You could even add to your web site along with the contact information: "Please report any suspected security violations or problems to **{contact name}**".

Notifying Employees of Incidents

When appropriate, notify your employees of known suspicions and incidents.

6.1.1 Evidence

When an incident occurs, you must gather the facts of what happened, how it happened, and note any indicators or trails that can help in the investigation. Lack of a clear trail of evidence when investigating any ISS crime is critical. Without proper evidence, you may be prevented from taking legal action.

Collecting Evidence

If possible, do whatever you can to quickly gather evidence of what you are witnessing or detecting. Do not let this task interfere or slow down the reporting process. For example, you may want to write down peculiar system performances, error messages to help the investigation.

Preserving Evidence

If possible, you should preserve the evidence for further investigation. For example, you should leave important system messages on the screen and not erase important information. This should only be done if it doesn't interfere with business resumption or if it doesn't cease the attack.

Recording Evidence

All suspicions and incidents should be carefully documented. This includes recording examples of the evidence, attaching screen shots, system printouts, and any other such system supporting evidence.

Annexure A: Security Policy Guidelines

6.1.2 Incident Response

The most important thing to remember is to be PROMPT.

All information security suspicions and incidents must be reported as quickly as possible through your organization's proper internal channels. If problems and violations go unreported, they may lead to much greater losses for the organization than would have been incurred, had the problems been reported right away. Delays in reporting can mean massive additional losses for the organization.

Internal Response

This response reporting structure is internal to your organization and includes the following:

- Security department
- Help desk
- The manager
- Security guard
- Information owners
- IS system administrators
- Add others

Initially problems should be reported internally rather than externally, reducing any adverse publicity or loss announcements. External response reporting should only be done in an extreme emergency.

Centralized Response

It is sometimes necessary to centralize the ISS department to better control ISS issues. This department may include those not on the incident response team.

The reporting process can be to a central group such as the Help desk as opposed to line management or a service provider. The reporting process should not always go through management, since this additional step takes longer and is likely to delay corrective actions.

You can establish a centralized Information Security Department as the focal point for all reports of suspicions and incidents. In many organizations, these reports go only to lower level managers (such as department managers), and never find their way back to a centralized group. Unless there is centralized reporting, no loss history can be compiled, no loss analysis can be conducted, and no related decision-making can be performed. Centralized reporting is also useful for the mobilization of a computer emergency response team (CERT), an organization-wide contingency plan, and other important defensive resources. It also alleviates the reporting party's concerns about short-circuiting the chain of command.

External Response

Information describing security problems is valuable and certain government regulations (such as those pertaining to commercial banks in the United States) may require the reporting of information security problems to government regulators. In all cases the Security Agency MUST be informed.

If criminal action is suspected, the organization must contact the appropriate law enforcement and investigative authorities as quickly as possible.

Annexure A: Security Policy Guidelines

While internal reporting is to be encouraged and required, external reporting is sometimes necessary and includes the following:

- Law enforcement, police
- Fire department
- External auditors
- Outside authorities / local and national organizations such as the proposed Government Security Agency

If required by law or regulation, management must promptly report information security violations to external authorities. If no such requirement exists, in conjunction with representatives from the Legal Department, the Security Department, the Security Agency and the Internal Audit Department, management must weigh the pros and cons of external disclosure before reporting incidents. (In all cases, the Security Agency is considered an Internal Agency). Many organizations still refrain from reporting computer crimes because the public embarrassment, cost, and diversion of staff resources appear to outweigh the benefits. Benefits include setting an example to discourage other violations, giving employees the impression that management believes in the criminal justice system, and obtaining restitution. It is often desirable that management be given the ability to choose to report violations on case-by-case basis. Some organizations may wish to establish a committee that will evaluate the merits of external reporting on a case-by-case basis. As it stands, a significant number of computer crimes go unreported, and a significant number go undetected.

6.1.3 Investigating Incidents

Conducting Internal Investigations

Until charges are pressed or disciplinary action taken, all investigations of alleged criminal or abusive conduct must be kept strictly confidential to preserve the reputation of the suspected party.

Whenever evidence clearly shows that your organization has been victimized by a computer or communications crime, a thorough investigation must be performed. This investigation must provide sufficient information so that management can take steps to ensure that: (1) such incidents will not be likely to take place again, and (2) effective security measures have been reestablished.

Documenting the Incident

Documenting the incident is critical for the investigation and also to track future similar attacks. Someone should be designated to the task of preparing and maintaining all incident reports. All documentation should be restricted to the facts.

The written report(s) should include:

- Incident Summary
- Detailed Technical Summary
- Relevant logs
- Details on systems compromised (hardware/ os)
- Source of vulnerability exploited
- List of individuals involved

Annexure A: Security Policy Guidelines

6.1.4 Incident Reporting Form

All employees should have an Incident Reporting Form to capture the events they have witnessed. A format for this form is attached.

Incident Reporting Retention

Information describing all reported information security problems and violations must be retained for a period of time, usually around 3 years. In all cases, if the misdemeanor is associated to the actions of an employee or internal actor, the record must be permanently retained.

Incident Follow Up

You must follow up on all reported incidents or suspicions. Without a good follow up process in place, you will discourage your employees from future reporting.

6.1.5 Enforcement

Enforcement is sometimes difficult in a working environment, but without enforcement the policies and procedures you have put in place with your ISS program may not be taken seriously.

It is up to your organization to determine how and when to take action on an employee that has violated a rule. Even if the violation was an accident, you may still want to take action in the form of a warning or other corrective activity. Giving out "security tickets" can be effective.

Legal Responsibility

Perpetrators of crime should be prosecuted by the organization to the full extent of the law. Suitable procedures should be developed to ensure the appropriate collection and protection of evidence for these purposes. In order to prosecute successfully, proof is required and can be difficult to obtain unless the organization's information systems have adequate controls and audit capabilities.

6.1.6 Incident Handling

If an incident is reported, the Security Officer must follow these steps:

- Verify that it is indeed an incident
- Follow the general procedures for responding to incidents
- Notify the Incident Response Team
- Analyze the intrusion
- Communicate with all appropriate parties
- Set up barriers to block the intrusion (if possible)
- Image target system(s) and securely retain the information
- Investigate the incident by reviewing system logs and other monitor information
- Formulate a trail leading back to the source.
- Synchronize the activities on different systems, if possible.
- Apply short-term solutions to contain an incident

Annexure A: Security Policy Guidelines

- Eliminate all means of vulnerability
- Return systems to normal operation (after evidence is gathered)
- Determine if outside help required
- Collect and protect evidence
- Gather accurate loss data
- Document the incident
- Recover from the incident
- Follow up on the incident
- Focus on all communications, internal and external
- Take appropriate measures to secure your system against this happening again
- Notify law enforcement through proper channels

Closure:

- Identify and implement security lessons learned
- Hold a post mortem analysis and review meeting with all involved parties. Do this within three to five working days of completing the investigation of an intrusion.
- Prepare a final report for senior management and the Security Agency. This ensures awareness of security issues. Incidents should be reported no later than 5 working days after returning systems to normal operation.
- Revise security plans and procedures and user and administrator training to prevent future incidents. Include any new, improved methods resulting from lessons learned.
- Determine whether or not to perform a new risk analysis based on the severity and impact of an intrusion.
- Take a new inventory of your system and network assets.
- Participate in investigation and prosecution, if applicable.

Annexure A: Security Policy & Guidelines

6.1.7 Implementing an Incident Program

Suggested action Plan

- Assemble / educate the Incident Response Team
- Complete the Incident Response Chart as shown below
- Have periodic practice drills
- Implement an Incident Reporting Form
- Have procedure for mobilizing the team

To Report...	Comments	Procedure
... an incident in process.		Call ...
... sensitive information that has been or is being disclosed, lost, or damaged.		Call ...
... a software/ system malfunction.	Do not attempt a recovery yourself.	Note (if time) any error messages, unusual system behavior (how is it behaving differently than before?) Stop using the computer. Disconnect from any attached networks. Call ...
... a virus.		Shut down the involved computer. Disconnect from all networks. Call ...
... an offensive e-mail, call, etc.		Respond directly to the originator. If the originator does not promptly stop sending offensive messages, report it to ...
... suspicious behavior.		Call ...
... known systems security vulnerabilities, risks, alerts, and warnings.		Call ...
... equipment damage or loss.		Call ...
... a physical access violation.		Call ...

COMPUTER INCIDENT REPORTING SHORT FORM

Use this form to report incidents to the Government Security Agency. This form also outlines the basic information that law enforcement needs on a first call.

STATUS

- Site Under Attack Past Incident Repeated Incidents, unresolved

CONTACT INFORMATION

Name _____ Title _____
Organization _____
Direct-Dial Phone _____ E-mail _____
Legal Contact Name _____ Phone _____
Location/Site(s) Involved _____
Street Address _____
City _____ Region _____
Main Telephone/Mobile _____ Fax _____
ISP Contact Information _____

INCIDENT DESCRIPTION

- | | |
|--|--|
| <input type="checkbox"/> Denial of Service | <input type="checkbox"/> Misuse of Systems (internal or external)
(Includes inappropriate use by employees) |
| <input type="checkbox"/> Distributed Denial of Service | <input type="checkbox"/> Probe/Scan |
| <input type="checkbox"/> Intrusion/Hack | <input type="checkbox"/> Unauthorized Electronic Monitoring (sniffers) |
| <input type="checkbox"/> Malicious Code (virus, worm) | <input type="checkbox"/> Website Defacement |
| <input type="checkbox"/> Other (specify) _____ | |

Annexure A: Security Policy & Guidelines

DATE/TIME OF INCIDENT DISCOVERY

Date _____ Time _____

Duration of Attack _____

IMPACT OF ATTACK

- Loss/Compromise of Data
- System Downtime
- Damage to Systems
- Other Organizations' Systems Affected
- Financial Loss (estimated amount: RwFr _____)
- Damage to the Integrity or Delivery of Critical Goods, Services or Information

SEVERITY OF ATTACK, INCLUDING FINANCIAL LOSS OR INFRASTRUCTURE

- High
- Medium
- Low
- Unknown

SENSITIVITY OF DATA

- High
- Medium
- Low
- Unknown

How did you detect This? _____

Have you contacted law enforcement about this incident before? Who & when? _____

Has the incident been resolved? Explain _____

Information Systems Administrator's Incident Reporting Form

6.1.8 Point of Contact Information

Name	
Title	
Telephone/Fax Numbers	
Email	
Agency	

B. Incident Information

1. Background Information:	
a. Agency (if same as above, enter "SAME":	
b. Physical Location(s) of affected computer system/network (be specific):	
c. Date/time of the incident:	
d. Duration of the incident:	
e. Is the affected system/network critical to the agency's mission? (Yes/No)	

Annexure A: Security Policy & Guidelines

2. Nature of Problem (check all that apply):	
a. Intrusion	
b. System impairment/denial of access	
c. Unauthorized root access	
d. Web site defacement	
e. Compromise of system integrity	
f. Hoax	
g. Theft	
h. Damage	
i. Unknown	
j. Other (provide details in remarks)	
k. REMARKS:	

3. Has your agency experienced this problem before? (Yes/No; If yes, please explain in the remarks section.)
a. REMARKS:

Annexure A: Security Policy & Guidelines

4. Suspected method of intrusion/attack:	
a. Virus (provide name, if known)	
b. Vulnerable exploited (explain)	
c. Denial of Service	
d. Trojan Horse	
e. Distributed Denial of Service	
f. Trapdoor	
g. Unknown	
h. Other (Provide details in remarks)	
i. REMARKS:	

5. Suspected perpetrator(s) or possible motivation(s) of the attack:	
a. Insider/Disgruntled Employee	
b. Former employee	
c. Other (Explain remarks)	
d. Unknown	
e. REMARKS:	

6. The apparent source (IP address) of the intrusion/attack:
--

7. Evidence of spoofing (Yes/No/Unknown)
--

8. What computers/systems (hardware and software) were affected (Operating system, version):	
a. Unix	
b. Linux	
c. Windows Servers NT/2000/ 2003	
d. Windows Desktops 98/XP/2000 Pro	
e. Other (Please specify in remarks)	
i. REMARKS:	

9. Security Infrastructure in place. (Check all that apply)
--

Annexure A: Security Policy & Guidelines

a. Incident/Emergency Response Team	
b. Encryption	
c. Firewall	
d. Secure Remote Access/Authorization Tools	
e. Intrusion Detection System	
f. Security Auditing Tools	
g. Banners	
h. Packet filtering	
i. Access Control Lists	
j. REMARKS:	

Annexure A: Security Policy & Guidelines

10. Did intrusion/attack result in a loss/compromise of sensitive or information classified as private?	
a. Yes (provide details in remarks)	
b. No	
c. Unknown	
d. REMARKS:	

11. Did the intrusion/attack result in damage to system(s) or data?	
a. Yes (provide details in remarks)	
b. No	
c. Unknown	
d. REMARKS:	

12. What actions and technical mitigation have been taken?	
a. System(s) disconnected from the network?	
b. System Binaries checked?	
c. Backup of affected system(s)?	
d. Log files examined?	
e. Other (Please provide details in remarks)	
f. No action(s) taken	
g. REMARKS:	

13. Has law enforcement been notified? (Check all that apply.)	
a. Yes-local law enforcement	
b. Not	
c. REMARKS:	

14. Has another agency/organization been informed as assisted with the response?	
a. Yes-Security Agency	
b. Yes-Specify	

Annexure A: Security Policy & Guidelines

c. REMARKS:	

15. Additional Remarks:

--

If the reported incident is a criminal matter, you may be contacted by law enforcement for additional information.

Closure Information (Optional, Except 9 & 10)

1. (Optional) Did your detection and response process and procedures work as intended? If not, where did they not work? Why did they not work?

--

2. (Optional) Methods of discovery and monitoring procedures that would have improved your ability to detect an intrusion.

--

3. (Optional) Improvements to procedures and tools that would have aided you in the response process. For example, consider using updated router and firewall filters, placement of firewalls, moving the compromised system to a new name or IP address, or moving the compromised machine's function to a more secure area of your network.

--

4. (Optional) Improvements that would have enhanced your ability to contain an intrusion.

--

Annexure A: Security Policy & Guidelines

5. (Optional) Correction procedures that would have improved your effectiveness in recovering your systems.

--

6. (Optional) Updates to policies and procedures that would have allowed the response and recovery processes to operate more smoothly.

--

7. (Optional) Topics for improving user and system administrator preparedness.

--

8. (Optional) Areas for improving communication throughout the detecting and response processes.

--

Annexure A: Security Policy & Guidelines

9. (Required) A description of the costs associated with an intrusion, including a monetary estimate if possible.

--

10. (Required) Summary of post mortem efforts.

--