CONSTITUENCY DEVELOPMENT FUND BOARD

INFORMATION AND COMMUNICATION (ICT)

SECURITY POLICY

Document Control

Date	Version	Initials	Comments
May 2011	1.0	S.O.	Policy by Crona Communications
March 2012	2.0	J.K.K	CDF Board ICT Department

Document Distribution

Name	CDFB	Address	Version

Table of Contents

DOCUMENT CONTROL 1
DOCUMENT DISTRIBUTION 2

ACRONYMS 8

1.0 FOREWARD 9

2.0 EXECUTIVE SUMMARY 10

END USER COMPUTING POLICY AND PROCEDURE RESPONSIBILITY 10
Information and Communication Technology Department 10
Internal Audit Department 10
2.1 CRITICAL BUSINESS FUNCTION 11
2.2 SUPPORTING BUSINESS OBJECTIVES 11
2.3 CONSISTENT COMPLIANCE ESSENTIAL 11
2.4 TEAM EFFORT REQUIRED 11
2.5 INFORMATION SECURITY RESPONSIBILITIES 11
2.5.1 Information Owners 11
2.5.2 Employees Manager 12
2.5.3 Information Custodians 12
2.5.4 Information Users 13
2.5.5 Information Security Team 13
2.5.6 Internal Audit Department 13
2.5.7 Identifying Risks 13
2.5.8 Managing and Controlling Identified Risks 13
2.6 INFORMATION SENSITIVITY CLASSIFICATION 14
2.6.1 Classification 14
2.6.2 Handling Instructions 14
2.7 ACCESS CONTROL 14
2.7.1 Access Philosophy 14
2.7.2 Access Approval Process 14
2.7.3 Default Facilities 14
2.7.4 Unique User-IDs 14
2.7.5 Privilege Deactivation 15
2.7.6 User Authentication 15
2.8 PASSWORD MANAGEMENT 15
2.8.1 Choosing Passwords 15
2.8.2 Changing Passwords 16
2.8.3 Protecting Passwords 17
2.9 PRIVACY 17
2.9.1 Expectations of Privacy 17
2.9.2 Third Party Information Privacy 17
2.9.3 Public Statements 17
2.9.4 Non-Disclosure Agreements 18
2.9.5 Third Party Non-Disclosure Agreements 18
2.10 ACCEPTABLE USE OF THE INTERNET 18
2.10.1 Not a Fringe Benefit 18
2.10.2 Information Reliability 18
2.10.3 Posting Information to Discussion Groups 18
2.10.4 Downloading Software 18
2.10.5 Sending Security Parameters 18
2.10.6 Setting up Extra Services 18
2.10.7 User Anonymity 19
2.10.8 False Security Reports 19
2.10.9 Establishing Network Connections 19
2.10.10 Dial-Up Access 19

2.11 ELECTRONIC MAIL....19
2.11.1 Sharing and Forwarding....20
2.11.2 Message Recording....20
2.11.3 Harassing or Offensive Messages....20
2.11.4 Expectation of Privacy....20
2.11.5 Appropriate Use....21
2.11.6 Other General Guidelines....21
2.11.7 Security 22
2.11.8 Legal Implications....22
2.12 PRINTING, EMBOSSING, COPYING AND FAX TRANSMISSION....22
2.12.1 Destruction of Waste Copies....22
2.12.2 Faxing Precautions....23
2.12.3 Printer Precautions....23
2.12.4 Repair Services....23
2.13 VIRUSES, MALICIOUS SOFTWARE, AND CHANGE CONTROL....23
2.13.1 Virus Checking....23
2.13.2 If A Virus Is Detected....24
2.13.3 Change Control....24
2.14 PERSONAL USE OF INFORMATION SYSTEMS....24
2.14.1 Personal Use....24
2.14.2 Testing Prohibition....24
2.15 INTELLECTUAL PROPERTY RIGHTS....24
2.15.1 Legal Ownership....24
2.15.2 Making Copies of Software....24
2.16 SYSTEMS DEVELOPMENT....24
2.16.1 Production System Definition....24
2.16.2 Special Production System Requirements....25
2.16.3 Separation between Production, Development, and Test Systems....25
2.16.4 User Programming....25
2.17 ETHICS POLICY....25
2.17.1 Executive Commitment to Ethics....25
2.17.2 Employee Commitment to Ethics....26
2.17.3 Company Awareness....26
2.17.4 Maintaining Ethical Practices....26
2.17.5 Unethical Behavior....26
2.18 REPORTING PROBLEMS....26
2.18.1 What To Report....26
2.18.2 How to Report....26
2.19 NON-COMPLIANCE....26
3.0 INFORMATION OWNERSHIP POLICY....27
3.1 NEW CENTRALITY OF INFORMATION....27
3.2 POLICY SCOPE AND APPLICABILITY....27
3.3 ROLES AND RESPONSIBILITIES OF OWNERS....27
3.4 ROLES AND RESPONSIBILITIES OF CUSTODIANS....27
3.5 ROLES AND RESPONSIBILITIES OF USERS....28
3.6 MULTIPLE ROLES AND RESPONSIBILITIES....28
3.7 DESIGNATING OWNERS....28
3.8 DESIGNATING CUSTODIANS....28
3.9 DESIGNATING USERS....29
3.10 CHANGES IN STATUS....29
3.11 HANDLING OF INFORMATION FOLLOWING STATUS CHANGES....29
3.12 EXTERNALLY-SUPPLIED INFORMATION....29
3.13 SYSTEM-OF-RECORD....29
3.14 RISK ACCEPTANCE PROCESS....30
4.0 DATA CLASSIFICATION POLICY....30

4.1 INTRODUCTION AND OVERVIEW 30
4.1.1 Worker Responsibility *30*
4.1.2 Addresses Major Risks *30*
4.1.3 Consistent Approach Required *30*
4.1.4 Applicable Information *31*
4.2 ACCESS CONTROL 31
4.2.1 Need to Know *31*
4.2.2 System Access Controls *31*
4.2.3 Access Granting Decisions *31*
4.2.4 No Read up Permissions *31*
4.3 CLASSIFICATION LABELS 31
4.3.1 Owners and Production Information *31*
4.3.1 (a) CONFIDENTIAL *32*
4.3.1(b) PUBLIC *32*
4.3.2 Owners & Access Decisions *32*
4.4 LABELING 32
4.4.1 Consistent Classification Labeling *32*
4.4.2 Information Collections *32*
4.4.3 Storage Media *32*
4.4.4 Additional Public Information Labels *33*
4.4.5 Dictation Machines and Tape Recorders *33*
4.5 THIRD PARTY INTERACTIONS 33
4.5.1 Third Parties and the Need to Know *33*
4.5.2 Disclosures to Third Parties and Non-Disclosure Agreements *33*
4.5.3 Disclosures from Third Parties and Non-Disclosure Agreements *33*
4.5.4 Prior Review *33*
4.5.5 Owner Notification *34*
4.6 HANDLING 34
4.6.1 Unattended Printing *34*

5.0 E-MAIL SECURITY POLICY 34

5.1 CDF BOARD PROPERTY 34
5.2 AUTHORIZED USAGE 34
5.3 DEFAULT PRIVILEGES 34
5.4 USER SEPARATION 34
5.5 USER ACCOUNTABILITY 34
5.6 USER IDENTITY 35
5.7 USE ONLY CDF BOARD ELECTRONIC MAIL SYSTEMS 35
5.8 RESPECTING PRIVACY RIGHTS 35
5.9 NO GUARANTEED MESSAGE PRIVACY 35
5.10 CONTENTS OF MESSAGES 35
5.11 STATISTICAL DATA 35
5.12 HANDLING ATTACHMENTS 35
5.14 MESSAGE FORWARDING 36
5.15 HANDLING ALERTS ABOUT SECURITY 36
5.16 PUBLIC REPRESENTATIONS 36
5.17 USER BACK-UP 36
5.18 PURGING ELECTRONIC MESSAGES 36
5.19 HARASSING OR OFFENSIVE MATERIALS 36
5.20 PAPER CONFIRMATION FOR CONTRACTS 37

6.0 FIREWALL POLICY 37

6.1 POLICY OBJECTIVE AND SCOPE 37
6.2 PLAYING THE ROLE OF FIREWALLS 37
6.3 DEFINED DECISION MAKER 37
6.4 DEFAULT TO DENIAL 37
6.5 REGULAR AUDITING 37

6.6 CONTINGENCY PLANNING....38
6.7 EXTERNAL CONNECTIONS....38
6.8 FIREWALL ACCESS MECHANISMS....38
6.9 FIREWALL ACCESS PRIVILEGES....38
6.10 DEMILITARIZED ZONES....38
6.11 DISCLOSURE OF INTERNAL NETWORK INFORMATION....38
6.12 SECURE BACK-UP....38
6.13 FIREWALL DEDICATED FUNCTIONALITY....39
6.14 FIREWALL CHANGE CONTROL....39
6.15 POSTING UPDATES....39
6.22 MONITORING VULNERABILITIES....39
6.23 FIREWALL PHYSICAL SECURITY....39

7.0 INTERNET POLICY....39

7.1 OPPORTUNITIES AND RISKS....39
7.2 APPLICABILITY....39
7.3 PRIOR MANAGEMENT APPROVAL....39
7.4 INFORMATION RELIABILITY....40
7.5 VIRUS CHECKING....40
7.6 PUSH TECHNOLOGY....40
7.7 SPOOFING USERS....40
7.8 USER ANONYMITY....40
7.9 ATTACHMENTS....40
7.10 WEB PAGE CHANGES....40
7.11 INFORMATION EXCHANGE....40
7.12 POSTING MATERIALS....41
7.13 EXTERNAL REPRESENTATIONS....41
7.14 APPROPRIATE BEHAVIOR....41
7.15 REMOVAL OF POSTINGS....41
7.16 DISCLOSING INTERNAL INFORMATION....41
7.17 INADVERTENT DISCLOSURE....41
7.18 COPYRIGHTS....42
7.19 BROWSER USER AUTHENTICATION....42
7.20 INTERNET SERVICE PROVIDERS....42
7.21 ESTABLISHING NETWORK CONNECTIONS....42
7.22 ESTABLISHING NEW BUSINESS CHANNELS....42
7.23 PERSONAL USE....42
7.24 BLOCKING SITES....42
7.25 MANAGEMENT REVIEW....43
7.26 LOGGING....43
7.27 JUNK E-MAIL....43
7.28 NOTIFICATION PROCESS....43
7.29 FALSE SECURITY REPORTS....43
7.30 TESTING CONTROLS....43

8.0 COMPUTER SECURITY POLICY....44

8.1 OBJECTIVES AND SCOPE....44
8.2 BUSINESS USE ONLY....44
8.3 CHANGES TO APPLICATION SOFTWARE....44
8.4 CHANGES TO OPERATING SYSTEM CONFIGURATIONS....44
8.5 CHANGES TO HARDWARE....44
8.6 VIRUS PROGRAM INSTALLED....44
8.7 DECOMPRESSION BEFORE CHECKING....45
8.8 ERADICATING VIRUSES....45
8.9 PLAYING WITH VIRUSES....45
8.10 ARCHIVAL COPIES....45
8.11 COPYRIGHT PROTECTION....45

8.12 DELETION OF OLD INFORMATION 45
8.13 DESTRUCTION OF INFORMATION 45
8.14 DOCUMENTATION FOR PRODUCTION SYSTEMS 45
8.15 EQUIPMENT THEFT 45
8.16 CUSTODIANS FOR EQUIPMENT 46
8.17 USE OF PERSONAL EQUIPMENT 46
8.18 PROPERTY PASS 46
8.19 POSITIONING DISPLAY SCREENS 46
8.20 ENVIRONMENTAL CONSIDERATIONS 46
8.21 PROCUREMENT OF ICT EQUIPMENT AND SOFTWARE 46
8.22 MAINTENANCE OF ICT EQUIPMENT 46
8.23 CDF BOARDING OF ICT EQUIPMENT 46
8.24 DISPOSAL OF ICT EQUIPMENT 47

9.0 NETWORK SECURITY POLICY 47

9.1 PURPOSE 47
9.2 SCOPE 47
9.3 SYSTEM ACCESS CONTROL 47
9.3.1 End-User Passwords 47
9.3.2 Password System Set-Up 48
9.3.3 Log-In/Log-Off Process 48
9.4 SYSTEM PRIVILEGES 49
9.4.1 Limiting System Access 49
9.4.2 Process for Granting System Privileges 49
9.4.3 Process for Revoking System Access 50
9.4.4. Establishment of Access Paths 50
9.4.5 Computer Viruses, Worms and Trojan Horses 51
9.4.6 Data and Program Back-up 51
9.4.7 Portable Computers 52
9.4.8 Remote Printing 52
9.4.9 Privacy 52
9.4.10 Logs and other systems security tools 53
9.4.11 Handling network security information 53
9.4.13 Physical security of computer and communication equipment 54
9.4.14 ICT Equipment Insurance 54
9.4.15 Exception 54
9.4.16 Violations 55

10. DATA BACKUP POLICY 55

10.1 Background 55
10.2 Purpose 55
10.3 Guidelines 55
10.3.1 Retention 55
10.3.1 Media Storage 56
10.3.2 Personnel-in-Charge 56
10.3.3 Training 56
10.3.3 Documentation 56
10.3.4 Restoration of Data 56
10.3.5 ICT Human Resource Development Policy 57
10.3.6 Capacity building 57

11. APPENDIX 61

Appendix I – Technology Resource Use Policy 61

ACRONYMS

BCM – Business Continuity Management
BCP - Business Continuity Plan
BIA - Business Impact Assessment
CDFB – Constituency Development Fund Board
HR - Human Resource
ICT - Information Communication Technology
ID - Identity
MCA – Mission Critical Activity
PC - Personal Company
RPO - Recovery Point Objectives

Definitions of Terms

ICT: Means technologies, including computers, telecommunication and audiovisual systems that enable the collection, processing, transportation and delivery of information and communications services to users.

ICT Policy: A policy is a plan of action to guide decisions and achieve results

User: A user means any person who is recognized by the CDF Board as having a valid reason to access the CDF Board's ICT Systems within or without.

Business Continuity Management: This is a holistic business approach that includes policies, standards, frameworks and procedures for ensuring that specific operations can be maintained or recovered in a timely fashion in the event of disruptions. Its purpose is to minimize the operations, financial, legal, reputational and other material consequences arising from disruptions.

Business Continuity Plan: This means a comprehensive, documented plan of action that sets out procedures and established the processes and systems necessary to continue or restore the operation of an organization in the event of a disruption.

Business impact Analysis: This means the process of identifying, and measuring quantitatively the business impact loss of business process in the event of a disruption.
It is used to identify recovery priorities, recovery resource requirements and essential staff to help shape the business continuity plan. All impacts should be measured on financial, regulatory, legal and reputational damage basis.

Communication protocols: This means an established procedure for communication that is agreed in advance between two or more parties internal or external to an institution. Such procedure also includes the nature of the information that should be shared with internal and external parties and how certain types of information should be shared with internal and external parties.

Critical services: It means any activity, function, process or services the loss of which would be material to the continued operations of a financial institution.

Crisis: It is an event, occurrence and/or perception that threat the operations, staff, shareholders value, stakeholders, brand, reputation trust and /or strategic/business goals of an institution.

1.0 FOREWARD

The growing dependence of Constituency Development Fund Board Secretariat (hereinafter referred to as CDF Board) on its information systems, coupled with the risks, benefits and opportunities, Information and Communications Technology (hereinafter referred to as ICT) carries with it, have made ICT governance an increasingly critical facet of overall governance. The Board and management, alike, need to ensure that ICT is aligned with CDF Board's strategies and CDF Board's strategies take proper advantage of ICT.

The management has a responsibility to ensure that the organization provides all users with a secure information systems environment. Furthermore, CDF Board needs to protect itself against the risks inherent in the use of information systems while simultaneously recognizing the benefits that accrue from having secure information systems. Thus, as dependence on information systems increases, so too does the criticality of information security, bringing with it the need for effective information security governance.

The objective of information security is "protecting the interests of those relying on information, and the systems and communications that deliver the information, from harm resulting from failures of *availability, confidentiality* and *integrity*."

In recognition of the critical role of information security, this policy defines the rules of and other requirements necessary for the secure and reliable operation of our information systems.

This policy also defines "baseline" control measures that everyone at CDF Board is expected to be familiar with and to consistently follow. Policies also define the minimum controls necessary to prevent legal problems such as allegations of negligence, breach of fiduciary duty, or privacy violation.

Safeguarding of the CDF Boards' assets is no longer the domain of the security department, but a team effort requiring a collective responsibility. It is therefore the duty of every employee, contractor or consultant to maintain the day-to-day security of its sites, systems and information. The management is indeed confident that everyone will exercise his/ her own responsibility to attain world-class security. Nothing short of this will be anticipated by stakeholders.

Chief Executive Officer

2.0 EXECUTIVE SUMMARY

CDF Board management shall, through an effective Information Security Program:

- Assure the security and confidentiality of records and information as well as the proprietary records and information of the CDF Board;
- Protect against any anticipated threats or hazards to the security or integrity of such records and information; and
- Protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to the CDF Board.

The program shall use appropriate administrative, technical, and physical safeguards to protect records and information as well as the CDF Board's own proprietary information.

End User Computing Policy and Procedure Responsibility

The senior management delegates the day-to-day management of the use of personal computers to the functional managers. They are responsible for ensuring that their employees adhere to the CDF Board's policies and procedures.

Information and Communication Technology Department

The Information and Communication Technology (hereinafter referred to as ICT) department is responsible for supporting and coordinating the day-to-day operation of the end user computing environment in a manner that is consistent and in compliance with the approved policies and procedures. Additionally, the ICT department should monitor and review the activities of end users to ensure that they are adhering to the CDF Board's ICT policies and procedures.

Internal Audit Department

The Internal Audit Department (hereinafter referred to as IAD) is responsible for conducting periodic reviews of the end user computing environment to ensure that policies and procedures are adequate to properly control the environment and that all end users consistently follow these policies and procedures.

The IAD also has the responsibility to evaluate the level of compliance with the CDF Board's ICT standards, policies, and procedures and to report any discrepancies to the appropriate department manager for correction and enforcement and to the board of directors through the audit committee in their regularly scheduled reports.

The IAD will be available to management, users, and the ICT department to provide input and recommendations in certain circumstances, including, but not limited to, the following:

- Purchase of new software
- Automation of procedures
- Access control issues
- Termination of employees
- Development and testing of systems/procedures
- Suspicion of fraud or misuse of software and/or hardware
- Implementation of new controls and/or testing

2.1 Critical Business Function

Information and information systems are necessary for the performance of every essential activity at CDF Board. If there were to be a serious security problem with this information or these information systems, the CDF Board would suffer serious consequences including losses and/or degraded reputation. As a result, information security must be a critical part of the CDF Boards' business environment.

2.2 Supporting Business Objectives

This information security requirements document has been prepared to ensure that CDF Board is able to support further growth of its business, as well as ensure a consistently high level of CDF Board, supplier, employee, and other service providers. This document also intends to support the CDF Board's reputation for high-integrity and high-quality business dealings with all Stakeholders/ suppliers. Because prevention of security problems is less expensive than correction and recovery, this document therefore helps in reducing costs in the long run.

2.3 Consistent Compliance Essential

An unauthorized exception to security measures can jeopardize users, the entire operations of the CDF Board, and even outside organizations who rely on our systems, therefore parties are required to exercise a minimum level of security. This document defines that minimum level of due care which in some case might conflict with other objectives such as improved efficiency and minimized costs. Top management has examined these tradeoffs and has decided that these minimum requirements defined are appropriate for all Employees. As a result and as a condition of continued employment, all Employees (employees, contractors, consultants, temporaries, etc.) must consistently observe the requirements set forth in this document.

2.4 Team Effort Required

Modern information and information systems are distributed to the office desktop, and are used in remote locations where the worker's role has become an essential part of information security. Information security is no longer the exclusive domain of the ICT department and thus requires the participation of every employee who comes into contact with information and/or information systems.

2.5 Information Security Responsibilities

The CDF Board's Secretariat Head of ICT Department is assigned primary responsibility for the development, implementation, and maintenance of the program.

2.5.1 Information Owners

CDF Board Chief Managers in user departments are the designated owner of all types of information used for business activities. However Information owners do not legally own the information in question; but are members of the management team who make decisions on behalf of the CDF Board. Information owners or their delegates are required to make the following decisions/ activities

1. Approve information-oriented access control privileges for specific job profiles,
2. Approve information-oriented access control requests which do not fall within the existing job profiles,

3. Select a data retention period for their information, relying on advice from the Legal/ Administration/Internal Audit Department/ICT Department
4. Designate a system-of-record (original source) for information from which all management reports will be derived,
5. Select special controls needed to protect information (such as additional input validation checks or more frequent back-up procedures),
6. Define acceptable limits on the quality of their information (accuracy, timeliness, time from capture to usage, etc.),
7. Approve all new and different uses of their information,
8. Approve all new or substantially enhanced application systems that use their information before these systems are moved into production operational status,
9. Review reports about system intrusions and other events which are relevant to their information,
10. Review and correct reports which indicate the current production uses of their information,
11. Review and correct reports which indicate the job profiles which currently have access to their information,
12. Select a sensitivity classification category relevant to their information and review this classification every five years for possible downgrading, and
13. Select a criticality category relevant to their information so that appropriate contingency planning can be performed.

Information owners can designate a back-up person to act if they are absent or unavailable. However owners may not delegate ownership responsibilities to third party organizations, such as outsourcing firms or to any individual who is not a full-time CDF BOARD employee. When both the owner and the back-up owner are unavailable, a decision may be made by the Departmental Head/Manager who ordinarily handles the information.

2.5.2 Employees Manager

Access control requests are approved by the employee's immediate manager based on the existing job profiles. If a job profile doesn't exist, it is the manager's responsibility to create one, after obtaining approval from the relevant owners, and informing the ICT department. Similarly, when an employee leaves CDF Board, it is the employee's immediate manager's responsibility to promptly advise the ICT department to revoke the privileges associated with the employee's user-ID/account. User-Ids/accounts are specific to individuals, and will not be reassigned to, or used by others. An employee's manager is additionally responsible for reassigning the involved duties and files to other employees.

2.5.3 Information Custodians

Custodians are in physical or logical possession of information and/or information systems. The Head of ICT, will be the custodian and will follow the instructions of the owners, operate systems on behalf of owners and also serve users authorized by owners. Custodians define the technical options, such as information criticality categories, and then allow owners to select the appropriate option(s) for their information. They also define information systems architectures and provide technical consulting assistance to owners so that information systems can be built and run to best meet the Board's objectives. If requested, custodians additionally provide reports to owners about information system operations, information security problems, and the like. Custodians are furthermore responsible for safeguarding the information in their possession, including implementing access control systems to prevent inappropriate disclosure, as well as developing, documenting, and testing information systems contingency plans.

2.5.4 Information Users

Users are any worker with access to internal information or internal information systems. Users are required to abide by all security requirements defined by owners, implemented by custodians, and/or established by the ICT department. Users are also required to participate in information security training and awareness program. Users must request access from their immediate manager, and report all suspicious activity and security problems.

2.5.5 Information Security Team

The Information Security Team is the central point of contact for all information security matters at CDF Board. It is responsible for creating workable information security compromises, which take into consideration the needs of Users, Custodians and Owners. This team defines the information security standards, procedures, policies, and other security requirements applicable to the CDF Board. The Information Security Team is also responsible for handling all access control administration activities, monitoring the security of information systems, and providing information security training and awareness programs to all the Employees. The team is additionally responsible for periodically providing the management with reports/ returns about the state of information security and providing assistance related to emergency response procedures and disaster recovery. The Information Security Team is also responsible for organizing a computer emergency response team to promptly respond to virus infections, hacker break-ins, system outages, and similar information security problems. The Information Security Team consists of team members from the following departments: ICT, Internal Audit, Finance, Programmes, Administration and Human Resource. The team will be led by a nominated team leader.

2.5.6 Internal Audit Department

The Internal Audit Division periodically performs compliance checks to make sure that the above-mentioned parties are performing their assigned duties, and to make sure that other information security requirements are being consistently observed to the top management expectations.

2.5.7 Identifying Risks

Management shall identify the reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of information or information systems. Further, management shall develop and implement procedures and other controls that take into account the likelihood and potential damage of these threats.

2.5.8 Managing and Controlling Identified Risks

Management shall develop, implement, and maintain the Program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the CDF Board's activities.

Management has, as of today, identified the following security measures appropriate for the CDF Board and either has or will shortly adopt those measures that management concludes are appropriate. Testing methods are also listed.

2.6 Information Sensitivity Classification

2.6.1 Classification

A classification hierarchy is used to handle information security according to its sensitivity. One important intention of a sensitivity classification system is to provide consistent handling of the information, no matter what form it takes, no matter where it goes, and no matter who possesses it. For this reason, it is important to maintain the labels reflecting sensitivity classification categories. CDF Board uses two sensitivity classification categories

Public – All information approved for public release by CEO, which includes brochures, and material posted to the CDF Board's web-site.

Confidential – All other information is sensitive in nature and must be restricted to those with a legitimate business need to access. Unauthorized disclosure of information to people without a business need for access may be against laws and regulations, or may cause significant problems to the CDF Board, or partners.

2.6.2 Handling Instructions

All Users must observe the requirements for handling information based on its sensitivity. Owners may designate additional controls to further restrict access to, or to further protect their information.

2.7 Access Control

2.7.1 Access Philosophy

Access to information in CDF Board will be provided on "a need to know and event by event basis" i.e. information shall be disclosed only to bona fide people who have business needs. Access will be granted only after obtaining approval from the information owner.

2.7.2 Access Approval Process

Access control approval process is initiated by an Employees' manager, and the privileges granted correspond with the user's job description and will remain in effect until the worker's job changes or the worker leaves the CDF Board. If either of these two events takes place, the manager must immediately notify the Head of ICT.

2.7.3 Default Facilities

All users will be granted basic information systems services such as electronic mail and personal computer facilities. All other system capabilities will be provided via job profiles or by special request directed to the owner of the involved information. If users have any questions about access control privileges, they should direct these questions to the Information Security Team or ICT department.

2.7.4 Unique User-IDs

Each User will be assigned their own unique user-ID/accounts, which shall be used by the individual as they move through the CDF Boards hierarchy until permanently CDF Boarded when a user leaves CDF Board. Every user-ID and related password is intended for the exclusive

use of a specific individual and must never be shared with anyone. User-IDs are linked to specific people and anonymous user-IDs (such as "guest") are not allowed and will be removed completely.

2.7.5 Privilege Deactivation

Users must be sure to log-off from multi-user computers when they leave their desks for any more than thirty (30) minutes. Users who come back from an extended vacation or a leave of absence must contact their manager and ICT department for reestablishment of their privileges.

2.7.6 User Authentication

Users are responsible for all activity that takes place with their user-ID and password (or other authentication mechanism). Users must immediately change their password if they suspect that it has been discovered or used by another person. Likewise, Users must notify the Information Security Team or ICT department if other access control mechanisms are broken or if they suspect that these mechanisms have been compromised.

2.8 Password Management

Passwords are unique strings of characters that employees provide in conjunction with a User ID, to gain access to an information resource. Passwords are an important aspect of information security because they are the first line of defense in protecting CDF Board information. Passwords are intended to be difficult to guess but still easy to remember. A poorly chosen password may result in the compromise of confidential information that could adversely affect both the CDF Board.

All employees are responsible for taking the appropriate steps to select and secure their passwords. This section establishes best practices for password selection as well as protection and use of passwords.

2.8.1 Choosing Passwords

CDF Board employees use passwords to access various resources. These resources include access to personal computers, the network, ERP, the Internet, and Email etc. User IDs and passwords are used to authenticate employees to the particular resource and are used to track user activity while using that resource. Temporary passwords are usually assigned to employees when access is initially granted to a resource. It then becomes the employee's responsibility to establish a strong secure password.

Employees must be aware of the characteristics of strong and weak passwords in order to ensure adequate protection of CDF Board and customer information. If someone obtains an employee's User ID and password, that individual can imitate the employee without the system knowing. Any damage created by the intruder will appear to have been created by the employee.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters;
- The password is a word found in a dictionary;
- The password is a common usage word such as:

- Names of family, pets, friends, co-Employees, sports, teams, movies, shows, license plate number, birth dates, etc.;
- Computer terms and names, commands, sites, companies, hardware, software;
- The words CDF Board, etc.;
- Birthdays, PIN number, User ID and other personal information such as addresses and phone numbers;
- Word, number or keyboard patterns like "aaabbb," "qwerty," "123321;"
- Repeating patterns like SwC@QE1, SwC@QE2, SwC@QE3, etc.;
- Any of the above preceded or followed by a digit (i.e., "CDF Board03");
- Any of the above spelled backwards; or,
- All the same characters or digits, or other commonly used or easily guessed formats.

Strong passwords have the following characteristics:

- Contains 2 characters from the following four groups:

Group	Examples
Uppercase letters	A, B, C ...
Lowercase letters	a, b, c ...
Numerals	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Symbols found on the keyboard (all keyboard characters not defined as letters or numerals)	` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /

- Have digits and punctuation characters as well as letters;
- Are at least eight characters long;
- Are not a word in any language, dictionary, slang, dialect, jargon, etc.; and,
- Are not based on personal or company information e.g. user name, company name, department name, names of family, etc.

Employees should refrain from writing down the password. Instead, employees should create passwords that can be easily remembered. One way to accomplish this is to create a password based on a song title, affirmation or other phrase. For example, the phrase might be "every day I write the book" and the password could be "ED1rtb@@k" or some other variation.

2.8.2 Changing Passwords

CDF Board policy requires passwords to be changed regularly, but an employee may change a password at any time if there is a possibility that the password has been compromised. Generally, the CDF Board's various computer systems do not permit employees to reuse a previously used password for a minimum period of time, as defined by the system. The

network system prompts for password change every 45 days. To save time and effort, passwords should be changed before they expire.

If a password has been compromised or forgotten, the user may obtain a new password or have their password reset by contacting the ICT department.

For more information on password standards contact the ICT department.

2.8.3 Protecting Passwords

The following is a list of things that employees should NOT do:

1. Don't reveal your password over the phone to anyone – not even individuals who claim to be calling from the ICT Department;
2. Don't reveal your password in an e-mail message;
3. Don't reveal your password to your manager or any other CDF Board employee;
4. Don't talk about your password in front of others;
5. Don't hint at the format of a password (i.e., "my family name");
6. Don't reveal your password on questionnaires or security forms;
7. Don't share your password with family members;
8. Don't reveal your password to co-Employees while on vacation;
9. Don't leave your password anywhere on or near your workstation (i.e., post-it notes, under mouse pads, etc.); and,
10. Don't create passwords for group use or shared passwords. Passwords should be unique to each person.
11. Do not provide your password to anyone who requests or demands it. Refer the incident to the CDF Board's Head of ICT and call the ICT department immediately to change your password if you suspect that your password has been compromised.

2.9 Privacy

2.9.1 Expectations of Privacy

Users should have no expectation of privacy when using information systems at CDF Board. To manage systems and enforce security, the CDF Board will log, review, and capture User activity such as telephone numbers dialed and websites visited.

2.9.2 Third Party Information Privacy

A wide variety of third parties have entrusted their information to CDF Board for business purposes, and all Employees must do their best to safeguard the privacy and security of this information. The most important of these third parties is the suppliers; whose account data is confidential and access strictly limited based on business need for such access. Suppliers account information must not be distributed to other third parties.

2.9.3 Public Statements

To maintain confidence, all Employees who will be delivering speeches, attending interviews with the media or disclosing information about the CDF Board/or its business must obtain preauthorization from CEO . Only designated individuals are authorized to be spokespersons for the CDF Board.

2.9.4 Non-Disclosure Agreements

Whenever communications with third parties necessitate the release of sensitive information, a standard non-disclosure agreement (NDA) must be signed by the third party. Information released to these third parties must be limited to the topics directly related to the involved project or business relationship.

2.9.5 Third Party Non-Disclosure Agreements

In some instances, before discussions can be commenced, third parties will ask that Employees of CDF Board sign their NDA. Such third party NDA should be forwarded to the Legal department for their signature.

2.10 Acceptable Use of the Internet

2.10.1 Not a Fringe Benefit

Internet access will be provided only if necessary to perform a worker's job. If a User needs additional access to Internet facilities, a request should be directed to the User's manager, who in turn will contact the Head of ICT.

2.10.2 Information Reliability

All information taken off the Internet should be considered suspect until confirmed as there is no standard quality control process on the Internet, and a considerable amount of information on the Internet is outdated, inaccurate, and in some cases deliberately misleading or spoofed by anonymous user on the Internet. Users must not rely on the alleged identity of a correspondent on the Internet unless the identity of this person is confirmed through digital certificates or digital signatures.

2.10.3 Posting Information to Discussion Groups

Users must not post to public discussion groups, chat rooms, or other public forums on the Internet unless they have been preauthorized by the CEO to make this type of representation on behalf of CDF Board.

2.10.4 Downloading Software

Users must not download software from the Internet unless specifically authorized to do so by the ICT department or Information Security Team. Users may download data files from the Internet, but must check these files for viruses before executing them (decompression and decryption, when they are used, must be performed first).

2.10.5 Sending Security Parameters

Users must not send any sensitive parameters such as credit card numbers; telephone calling card numbers, fixed passwords, or account numbers through the Internet unless the connection is encrypted.

2.10.6 Setting up Extra Services

Subscription to electronic mail distribution lists (also known as "news groups") is permissible. The establishment of any network connection with a third party (such as an "extranet") is

forbidden unless the Information Security Team has approved the controls associated with this connection.

2.10.7 User Anonymity

Users must not misrepresent, obscure, suppress or replace their own or another user's identity on the Internet or on any other CDF Board information system. In all instances, the user name, electronic mail address and related contact information must reflect the actual originator of a message or posting. The use of anonymous re-mailers or other identity hiding mechanisms is forbidden and is not in keeping with straight and honest communication. The use of web browsers, anonymous FTP log-ins, and other methods established with the expectation that users do not need to identify themselves is permissible.

2.10.8 False Security Reports

The Internet has been plagued with hoaxes alleging various security problems like viruses, which will erase hard drives. Many of these hoaxes take the form of chain letters, which request that the receiving party send the message to other people. All Users in receipt of information about system vulnerabilities should forward this information to the Information Security Team for appropriate action. Users must not redistribute system vulnerabilities.

2.10.9 Establishing Network Connections

Employees must not connect their own computers with CDF Board computers or networks without prior authorization from Head of ICT. Likewise, personally owned systems may not be used to process any business information unless the systems have first been approved for use by the Information Security Team.

Employees and vendors must not make arrangements to complete the installation of voice or data lines with any carrier, unless they have first obtained written approval from the CEO.

All connections between the CDF Boards' internal networks and the Internet must include an approved firewall or related access control system. The privileges that will be permitted via this firewall or related access control system will be based on business needs, and will be defined in an access control standard issued by the Head of ICT.

2.10.10 Dial-Up Access

All dial-up connections with CDF Board computers and networks must be approved by the Head of ICT.

2.11 Electronic Mail

The CDF Board grants e-mail capabilities to certain employees in order to provide an efficient manner of communication among CDF Board employees and with individuals outside the CDF Board. If used appropriately, e-mail has the potential to offer the following benefits to CDF Board employees:

- Encouragement of team work – particularly among individuals who are geographically dispersed;
- Cost-effective and environmentally-friendly means of day-to-day communication;

- Ability to disseminate information in a timely manner; and,
- Rapid delivery of administrative information to CDF Board personnel.

The use of e-mail also creates risks to the CDF Board that must be properly managed to ensure adequate protection of CDF Board assets as well as customer information. Risks created through the use of e-mail include:

- Inadequate awareness among e-mail users regarding the fact that e-mail is not a secure form of communication and that privacy and confidentiality are not guaranteed by the CDF Board;
- Delivery of inappropriate material to and from CDF Board e-mail accounts;
- Problems related to information overload when large quantities of information, some of marginal value, are delivered to individuals' e-mail accounts; and,
- Difficulty in controlling record keeping and legal liability issues.

2.11.1 Sharing and Forwarding

Electronic mail accounts, like user-IDs, are for specific individuals and must not be shared. Notices are established which will automatically notify correspondents that the recipient will not be responding for a certain period of time since the user has gone on a vacation. Upon departure, a User's electronic mail account is terminated.

Employees must exercise utmost caution when sending any e-mail from inside CDF Board to an outside network.

2.11.2 Message Recording

All electronic mail messages are recorded in logs and back-ups. This means that even though an electronic mail message may have been deleted from a User's in-box, it may still be retrievable with other methods. Messages that have been read will be purged from the systems every six (6) months; hence users are responsible for saving important messages, which might be needed at a future date in other storage places such as word processing documents.

2.11.3 Harassing or Offensive Messages

CDF Board information systems must not be used for the exercise of a User's right to free speech. Sexual, ethnic, and racial harassment -- including unwanted telephone calls, electronic mail, and internal mail -- is strictly prohibited and is cause for disciplinary action. Users are encouraged to respond directly to the originator of offensive electronic mail messages, telephone calls, and/or other communications. If the originator does not promptly stop sending offensive messages, Employees must report the communications to their manager and the Human Resources Department.

2.11.4 Expectation of Privacy

While CDF Board employees are provided with e-mail passwords, the use of such passwords is not intended to assure employees that e-mail communications will be kept confidential. The

CDF Board maintains the right to access any employee's e-mail communications and to retrieve stored e-mail information.

2.11.5 Appropriate Use

E-mail capabilities are provided strictly for business purposes. E-mails sent and received by CDF Board employees are considered CDF Board property. The use of e-mail via the CDF Board's facilities and/or equipment, by an employee, constitutes acknowledgment and understanding that the employee is representing the CDF Board. Incidental and occasional personal use of e-mail is permitted. However, such use will not be confidential and must comply with this section of the guide as well as any other CDF Board policies covering such use. Further, any incidental e-mail usage may not interfere with the employee's official duties and must have a minimal effect on the CDF Board.

2.11.6 Other General Guidelines

1. The e-mail system should not be used to communicate confidential CDF Board information to anyone outside the CDF Board.
2. CDF Board employees are prohibited from reading e-mail communications delivered to another CDF Board employee's mailbox without proper authorization from CDF Board management. Further, any employee who receives an e-mail communication intended for someone else must immediately inform the sender that the e-mail communication was sent to the wrong person. The employee must then delete the e-mail communication.
3. The e-mail system must not be used for any form of harassment, threat or any communication that could be deemed abusive, defamatory, obscene, offensive, derogatory or otherwise inappropriate, illegal or unrelated to CDF Board business. This includes a prohibition against e-mail communications that harass or offend on the basis of race, color, religious belief, sex, sexual orientation, national origin, ancestry, age, marital status, disability, mental condition or veteran status.
4. Employees may not use the e-mail system for the purpose of personal or non-CDF Board solicitations (i.e., spam, etc.). Examples include but are not limited to, anything in conjunction with an employee's outside endeavors or sales of any product or outside service (i.e., home products, cosmetics, etc.).
5. Employees may not use the e-mail system to deliver messages related to political issues (i.e., encouraging or advocating a certain position, bill, etc.) unless there is a compelling business reason. Prior approval must be obtained from management.
6. Messages that violate CDF Board policy or that are contrary to supervisory instructions are not permitted.
7. Personal announcements (i.e., items for sale, requests for roommates, etc.) are not permitted.
8. The e-mail system may not be used to create or forward "chain letters," "Ponzi" or "pyramid" schemes of any type.
9. Posting non-business-related messages to Internet newsgroups using the CDF Board's e-mail account is prohibited.
10. Employees should exercise good judgment in the use of e-mail distribution lists (i.e. All, HQ, CDFFAMS etc.) these lists are developed for the convenience of the sender and unnecessary or frivolous messages should not be sent. Employees should limit the distribution of e-mail to the smallest group possible in order to eliminate unnecessary congestion on the CDF Board's computer network.

11. Employees should delete unwanted e-mail messages as soon as practical and should log off the e-mail system when leaving their workstation for an extended period of time.
12. Employees must avoid opening e-mail attachments received from unknown senders, which may contain viruses or other malicious computer programs.
13. Employees are prohibited from sharing with third parties the e-mail addresses of CDF Board employees for the purpose of marketing (i.e., spamming) to these employees.
14. Employees must not use their company e-mail address to sign up for non-business related Internet e-mail lists.
15. Employees have the responsibility of reporting to the Head of ICT in any case of misuse of e-mail resources.

2.11.7 Security

E-mail messages are not secure. Risks to e-mail include someone intercepting the message during transit or the message being inadvertently delivered to the wrong person. Another risk is someone forwarding a private/confidential e-mail to someone else. These risks are increased when e-mail is accessed /delivered through the use of Webmail.

As such, employees should never include anything in an e-mail message that is private or confidential or that could create the risk of litigation or otherwise put the CDF Board at risk. The following are some examples of information that should not be included in an e-mail:
Passwords;

- Confidential CDF Board information (when delivering an e-mail to an external party); or,
- CDF Board secrets, contracts, strategic plans, etc. (when delivering an e-mail to an external party).

2.11.8 Legal Implications

E-mail is a formal means of business communication. Erasing an e-mail does not necessarily erase all copies of the e-mail. Archived copies of the e-mail may reside for substantial periods of time, in the CDF Board's records. Archived copies of e-mails are subject to the same right to access as messages stored in an employee's mailbox. For these reasons, employees should refrain from including in an e-mail anything that they would not ordinarily include in a memorandum or state in the open or in a court of law.

Employees must be aware that e-mail is subject to the full range of laws and regulations that apply to other forms of communication. Applicable laws and regulations affect issues such as copyrights, anti-discrimination, defamation, privacy, harassment, etc.

The ease of use and ability to conveniently contact a larger group of individuals makes it possible to inadvertently break the law or breach security and privacy. Through the use of law, regulation or agreement, certain third parties including attorneys and government agencies, may require the CDF Board to grant them access to stored e-mail.

2.12 Printing, Embossing, Copying and Fax Transmission

2.12.1 Destruction of Waste Copies

If a printer, embosser, copier, or fax machine jams or malfunctions when printing sensitive information, the involved Users must not leave the machine until all copies of the sensitive information are removed or are no longer legible. All paper copies of sensitive information

must be disposed of by shredding or other methods approved by the Information Security Team Leader.

2.12.2 Faxing Precautions

Sensitive materials must not be faxed unless:

(1) an authorized staff member is on-hand at the time of transmission to properly handle the materials at the receiving site,
(2) the fax is sent to a locked room to which only authorized Employees have access, or
(3) A password-protected fax mailbox is used to restrict release to an authorized recipient who should confirm receipt promptly. To ensure their enforceability in court, third party signatures on contracts, purchase orders, and similar legal documents sent by fax must always be followed-up with an exchange of paper originals.

2.12.3 Printer Precautions

When printing sensitive information, the User must

(1) Be present at the printer at the time of printing to prevent the information from being revealed to unauthorized parties, or
(2) Direct the output to a printer inside an area where only authorized Employees are permitted to go.

2.12.4 Repair Services

Because modern fax machines, printers, embosser and copy machines may have storage areas and internal logs, which could contain sensitive information, the repair of these machines must only be performed by third party vendors who have signed a non-disclosure agreement (NDA).

2.13 Viruses, Malicious Software, and Change Control

2.13.1 Virus Checking

- Always ensure that your computer is running the corporate standard and supported Anti-Virus program. The Anti-Virus management program will be sending automatic updates to all computers connected to the CDF Board network. In case your anti-virus program is not up to date, please consult the ICT department immediately.
- NEVER open any files or macros attached to an e-mail from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete spam, chain, and other junk e-mail without forwarding, in line with CDF Board's Acceptable Use Policy.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan any external storage media (floppy diskette, USB flash disks, Memory Sticks etc.) from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.

2.13.2 If A Virus Is Detected

If Users obtain virus alerts, they must immediately disconnect from all networks and cease further use of the affected computer, and then call the ICT department to get technical assistance.

2.13.3 Change Control

Users are not permitted to install new or upgraded operating systems or application software on personal computers or other machines used to process CDF Board information. This allows the CDF Board to perform software license management, remote back up, and related functions on a centralized and coordinated basis. Users can, however, change the preferences on software packages, such as the fonts for a word processing package.

2.14 Personal Use of Information Systems

2.14.1 Personal Use

All User activity is subject to logging and subsequent analysis. Users must not perform any activity that could damage the reputation of CDF Board. The use of software licensed to CDF Board on a personal computer owned by a User is not authorized.

2.14.2 Testing Prohibition

Users must not test, or attempt to compromise any information security mechanism unless specifically authorized to do so by the Information Security Team Leader. Users are prohibited from possessing software or other tools that are designed to compromise information security (for example, password cracking software).

2.15 Intellectual Property Rights

2.15.1 Legal Ownership

All business information stored on or passing through the CDF Board's systems is owned by CDF BOARD.

2.15.2 Making Copies of Software

Users must not make copies of or use software unless the copies are in agreement with the vendor's license. All systems used to process the CDF Boards' information are licensed and the Information Systems Department will remove any software, which is not authorized. Questions about licensing should be directed to the Information Systems Department, which maintains documentation reflecting software licenses throughout the group. Making regular back-ups of software for contingency planning purposes is permissible

2.16 Systems Development

2.16.1 Production System Definition

Information systems which have been designated "production systems" is a system which has gone live and is regularly used to process information critical to the business. Although a production system may be physically situated anywhere, the production system designation is assigned by the respective head of department.

2.16.2 Special Production System Requirements

All software which runs on production systems must be adequately documented and tested before it is used for critical business. All production systems must have an access control system to restrict who can access the system as well as restrict the privileges available to these Users and also have designated Owners and Custodians.

2.16.3 Separation between Production, Development, and Test Systems

Separation between the production, development, and test environments should be in place to ensure that security is maintained in a much more rigorous way for the production system, while the other two environments can maximize productivity with fewer security restrictions. Development and test staff must not be permitted to have access to production systems. All security fixes provided by software vendors must also go through the testing process, and must be promptly installed. Application programmers must not be given access to production information. A formal and documented change control process must also be used to restrict and approve changes to production systems.

2.16.4 User Programming

Users are not permitted to write production computer programs. The construction of spreadsheet formulas, automatic execution scripts which are run when a system is booted or databases, is not considered programming for purposes of this document. Programmers must never embed user-IDs or readable passwords in any file.

2.17 Ethics Policy

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

CDF Board is committed to protecting employees, partners, and vendors of various Software Programs from illegal or damaging actions by individuals, either knowingly or unknowingly. When CDF Board addresses issues proactively and uses correct judgment, it will help set things straight.

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

2.17.1 Executive Commitment to Ethics

- Top management within CDF Board must set a prime example. In any business practice, honesty and integrity must be top priority for executives.
- Executives must have an open door policy and welcome suggestions and concerns from employees. This will allow employees to feel comfortable discussing any issues and will alert executives to concerns within the work force.
- Executives must disclose any conflict of interests regard their position within CDF Board.

2.17.2 Employee Commitment to Ethics

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

2.17.3 Company Awareness

- Promotion of ethical conduct within interpersonal communications of employees will be rewarded.
- CDF Board will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the company.

2.17.4 Maintaining Ethical Practices

- CDF Board will reinforce the importance of the integrity message and the tone will start at the top. Every employee, manager, director needs consistently maintain an ethical stance and support ethical behavior.
- Employees at CDF Board should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.
- CDF Board has established a best practice disclosure committee to make sure the ethical code is delivered to all employees and that concerns regarding the code can be addressed.

2.17.5 Unethical Behavior

- CDF Board will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications.
- CDF Board will not tolerate harassment or discrimination.
- Unauthorized use of CDF Board secrets, operational, personnel, financial, source code, & technical information integral to the success of CDF Board will not be tolerated.
- CDF Board will not permit impropriety at any time and will act ethically and responsibly in accordance with laws.
- CDF Board employees will not use assets or business relationships for personal use or gain.

2.18 Reporting Problems

2.18.1 What To Report

All Employees must promptly report any loss or severe damage to their hardware or software, all suspected compromises to information systems, any serious information security vulnerability known to exist or any suspected disclosure of sensitive information to the Information Security Team Leader.

2.18.2 How to Report

Please call or e-mail the ICT department at the CDF Board Secretariat.

2.19 Non-Compliance

Any infractions of these policies will not be tolerated and CDF Board will act quickly in correcting the issue if any of the policy is broken.

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

3.0 INFORMATION OWNERSHIP POLICY

3.1 New Centrality of Information

Information is no longer simply something, which supports the provision of a product or service. Information itself has become a product, which CDF Board now offers. Information has additionally become a critical and integral part of other products and services that CDF Board provides. The new centrality of information necessitates the establishment of new roles and responsibilities to properly manage and protect it. To this end, this policy defines the information security roles and responsibilities of owners, custodians, and users. Information security can no longer be a concern of technical specialists alone; it must instead be addressed by a large team of individuals. This team is made up of every CDF Board worker who comes into contact with CDF Board information and/or information systems.

3.2 Policy Scope and Applicability

This policy applies to the handling of all CDF Board production information, regardless of the origin of this information (client transactions, third party market research, etc.). "Production information" is information routinely used to perform important business activities or routinely used to support management decision-making. This policy applies no matter what information handling technology is used, no matter where the information resides, no matter how the information is employed to meet business needs, and no matter which users have access to the information. This policy applies to all CDF Board Head Office departments, branches and all subsidiaries.

3.3 Roles and Responsibilities of Owners

Information owners are senior managers (CDF Board employees) with the authority for acquiring, creating, and maintaining information and information systems within their assigned areas of control. Owners are responsible for categorizing the information for which they have been designated an owner using the classifications defined in the Data Classification Policy. Owners are additionally responsible for authorizing user access to information based on the need-to-know. To this end, owners must establish profiles regarding the categories of people who will be granted access to the information for which they are the designated owner; these policies must also specify the type of access that each such category of person will be granted. Owners must also make decisions about the permissible uses of information including relevant business rules. For example, owners must define the validation rules used to verify the correctness and acceptability of input data. These validation rules and other controls for protecting information must be formally approved in writing by the relevant owner before major modifications can be made to production application systems. Separately, owners must understand the uses and risks associated with the information for which they are accountable. This means that they are responsible for the consequences associated with improper disclosure, insufficient maintenance, inaccurate classification labeling, and other security related control deficiencies pertaining to the information for which they are the designated owner.

3.4 Roles and Responsibilities of Custodians

Information custodians are individuals (often staff within the ICT department) in physical or logical possession of information from owners. Custodians are charged with the provision of

information systems services consistent with the instructions of owners, including information security measures. Using physical and logical access control systems, custodians must protect the information in their possession from unauthorized access, alteration, destruction, or usage. Custodians are also responsible for providing and administering general controls such as backup and recovery systems. Custodians are likewise responsible for establishing, monitoring, and operating information systems in a manner consistent with policies and standards issued by the Information Security Team Leader. Furthermore, custodians must provide owners with regular reports indicating user and systems activities. Custodians are forbidden from changing the production information in their possession unless they have received explicit and temporary permission from either the owner or an authorized user.

3.5 Roles and Responsibilities of Users

Information users are individuals who have been granted explicit authorization to access, modify, delete, and/or utilize information by the relevant owner. Users must use the information only for the purposes specifically approved by the owner. Users must also comply with all security measures defined by the owner, implemented by the custodian, and/or defined by the Information Security Team. Users must additionally refrain from disclosing information in their possession (unless it has been designated as Public) without first obtaining permission from the owner. Users must additionally report to the Information Security Team Leader all situations where they believe an information security vulnerability or violation may exist. Users of personal computers have special responsibilities (for example relating to back-up and virus screening), which are defined in the Personal Computer Policy.

3.6 Multiple Roles and Responsibilities

It is likely that certain individuals will act in multiple capacities with respect to certain types of information. For example, an employee may be the creator of a new type of production information, which is stored in a desktop personal computer. In this case, the worker must, at least temporarily, act in the capacity of owner, custodian, and user. To achieve a more secure operating environment, in general the roles of owner, custodian, and user should be performed by separate individuals wherever production information has more than one user. Creators of new types of production information must promptly inform the Head of ICT, so that appropriate roles and responsibilities may be established and maintained.

3.7 Designating Owners

If there are several potential information owners, higher-level management must assign ownership responsibility to the Head of ICT of the business unit, which makes the greatest use of the information. When acting in his or her capacity of owner, this individual must take into consideration the needs and interests of other stakeholders which rely upon or have an interest in the information. With the exception of operational computer and network information, managers in the ICT department must not be owners for any information. An owner's roles and responsibilities may be delegated to any full-time manager in the owner's business unit. An owner's roles and responsibilities may not be assigned or delegated to contractors, consultants, or individuals at outsourcing firms or external service bureaus.

3.8 Designating Custodians

Management must specifically assign responsibility for the control measures protecting every major production type of information. Owners are responsible for identifying all those individuals who are in possession of the information for which they are the designated owner.

These individuals by default become custodians. Although special care must be taken to clearly specify security-related roles and responsibilities when outsiders are involved, it is permissible for custodians to be contractors, consultants, or individuals at outsourcing firms or external service bureaus.

3.9 Designating Users

Users may be employees, temporaries, contractors, consultants, or third parties with whom special arrangements (such as non-disclosure agreements) have been made. All users must be known to and authorized by owners. The security-relevant activities of all users must be tracked and logged by custodians. To allow proper privilege assignment and activity logging, users must always be specific individuals; Users must not be defined as departments, project teams, or other groups.

3.10 Changes in Status

Due to promotions, transfers, retirements, etc., the individuals who play the roles of information owners, custodians, and users will change on a regular basis. It is the responsibility of the local manager of all individuals to promptly report status changes to the Information Security Team Leader. Custodians must maintain access control systems so that previously provided user privileges are no longer provided whenever there has been a user status change. When a custodian has a change in status, it is the responsibility of the owner to promptly assign a new custodian, and to assist the new custodian with the assumption of tasks previously performed by the former custodian (including necessary training).

3.11 Handling of Information Following Status Changes

Users who change their status must leave all production information with their immediate manager. Soon after a user has a change of status, both computer-resident files and paper files must be reviewed by the user's immediate manager to determine who should be given possession of the files, and/or the appropriate methods to be used for file disposal or destruction. The manager must then promptly reassign the user's duties as well as specifically delegate responsibility for information formerly in the user's possession. It is this manager's responsibility to train the new user so that the new user is able to fully perform the tasks previously performed by the former user.

3.12 Externally-Supplied Information

In the course of normal business activities, CDF Board often takes possession of third party sensitive information. Whenever a non-disclosure agreement (NDA) has been signed, an internal CDF Board owner must be assigned for information so received. The head of the department utilizing the information is ordinarily designated as the owner. This third party information must also be labeled with the appropriate data classification category and treated as though it was CDF Board internal information with the same classification. The roles and responsibilities for custodians and users are also relevant to externally-supplied information.

3.13 System-of-Record

Each owner must designate a "system-of-record" which will serve as the most authoritative copy of the information under his or her care. Updates to this information must be made to the system-of-record before or at the same time that updates are made to other systems containing

this information. It is the owner's responsibility to ensure that all production copies of the information for which he or she is the designated owner are maintained with appropriate controls to ensure a reasonable degree of information accuracy, timeliness, and integrity.

3.14 Risk Acceptance Process

In rare circumstances, exceptions to information security policies and standards will be permitted if the information Owner, the Manager, Information Security Team Leader, and the Head of ICT, has all signed a properly completed risk acceptance form. In the absence of such management approval reflected on a risk acceptance form, all owners, custodians, and users must consistently observe relevant CDF Board information security policies and standards.

4.0 DATA CLASSIFICATION POLICY

4.1 Introduction and overview

4.1.1 Worker Responsibility

All Employees who have any type of access to either information or systems have an important information security role to play. They are, for instance, personally responsible for the protection of information which has been entrusted to their care. To simplify the protection of information, to minimize information protection costs, and to clarify information protection requirements, management has compiled, approved, and issued this policy. This document defines a conceptual model for viewing the sensitivity of information as well as required methods for protecting information based on its sensitivity classification. All Employees who come into contact with "sensitive" internal information are expected to familiarize themselves with this data classification system policy and to consistently use it in their business activities. "Sensitive" information is either "Confidential" or "Secret" information (the latter two quoted words are defined below). Although this policy provides overall guidance, to achieve consistent information protection, Employees will be expected to apply and extend these concepts to fit the needs of day-to-day operations.

4.1.2 Addresses Major Risks

CDF Board's data classification system, as defined in this document, is based on the well-known concept called "need to know." This term means that information is not disclosed to any person who does not have a legitimate and demonstrable business to receive the information. This fundamental concept, when combined with the policies defined in this document, will help to protect information from unauthorized disclosure, use, modification, and deletion.

4.1.3 Consistent Approach Required

A single lapse in information security can have significant long-term consequences. Consistent use of this data classification system is absolutely essential if sensitive information is to be adequately protected. Without the consistent use of this data classification system, CDF Board unduly risks loss of loss of public confidence, internal operational disruption, and excessive costs. The intention of this policy is thus to consistently protect sensitive information no matter what form it takes, no matter what technology is used to process it, no matter who handles it,

no matter where the information may be located, and no matter what stage in its lifecycle (creation, production usage, archival storage, destruction, etc.) the information may be.

4.1.4 Applicable Information

This data classification policy is applicable to all information in CDF Board's possession or under CDF Board's control. Confidential information entrusted to CDF Board by its, business partners, suppliers, and other third parties must be protected with this data classification policy. Employees are expected to protect third party information with the same care that they protect CDF Board information.

4.2 Access control

4.2.1 Need to Know

Every one of the policy requirements set forth in this document is based on the concept called "need to know." If a worker is unclear how the requirements set forth in this policy should be applied to any particular circumstance, he or she must conservatively apply the need to know concept. That is to say that information must be disclosed only to those people who have a legitimate business need for the information.

4.2.2 System Access Controls

All computer-resident information will be protected via access controls to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable. Traditional access control systems employ fixed passwords, but these are giving way to more secure technologies including dynamic passwords and biometrics. These access control packages must not only control access based on the need to know, they must also log which users accessed what sensitive data, and the time and date of such access.

4.2.3 Access Granting Decisions

Access to CDF Board information will be provided only after the written authorization of the information owner has been obtained. Custodians of the involved information must refer all requests for access to the relevant owners or their delegates. Standard templates of system privileges are defined for all job titles, and these privileges are approved in advance by owners. Special needs for other access privileges will be dealt with on a request-by-request basis.

4.2.4 No Read up Permissions

Employees who have been authorized to view information classified at a certain sensitivity level will be permitted to access only the information at this level and at less sensitive levels.

4.3 Classification labels

4.3.1 Owners and Production Information

All production information possessed by or used by a particular Department within CDF Board will have a designated owner. Production information is information routinely used to accomplish business objectives. Information owners are responsible for assigning appropriate sensitivity classifications as defined immediately below. Owners do not legally own the information entrusted to their care. They are instead designated members of the CDF Board management team who act as stewards who supervise the ways in which certain types of information are used and protected.

4.3.1 (a) CONFIDENTIAL

This classification label applies to sensitive business information which is intended for use within CDF Board. Its unauthorized disclosure could adversely impact the CDF Board, its, suppliers, business partners, and/or its employees. Information that some people would consider to be private is included in this classification. Examples include employee performance evaluations, strategic alliance agreements, unpublished internally-generated research, computer passwords; identity token personal identification numbers (PINs), strategic plans and internal audit reports.

4.3.1(b) PUBLIC

This classification applies to information which has been explicitly approved by CDF Board management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be freely disseminated without potential harm. Examples include service brochures, advertisements, job opening announcements, and press releases.

4.3.2 Owners & Access Decisions

Owners must make decisions about who will be permitted to gain access to information, and the use to which this information will be put. Owners must additionally take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of information.

4.4 Labeling

4.4.1 Consistent Classification Labeling

If information is sensitive (Confidential or Secret), from the time it is created until the time it is destroyed or declassified, it must be labeled (marked) with an appropriate data classification designation. Such markings must appear on all manifestations of the information (hardcopies, floppy disks, USB flash disks, CD-ROMs, etc.). Employees are forbidden from removing data classification system labels from sensitive information unless the permission of the owner has first been obtained.

4.4.2 Information Collections

Employees who create or update a collection of information are responsible for choosing an appropriate data classification label for the new collection. This label must be consistent with the decisions made by the relevant owners and generally should be the most restricted classification level found in the collection. For example, if a new database is being created, and if it contains Internal Use Only as well as confidential information, then the entire database must be classified as Confidential. Other examples of such collections include internally generated intelligence report, management decision background reports, and access-controlled intranet web-pages. At the time that it is being compiled, every worker creating a new collection of this nature must notify the involved information owner(s) about the creation of their new collection.

4.4.3 Storage Media

If information recorded on computer storage media with a higher sensitivity classification is moved to media with a lower sensitivity classification, then the media with the lower sensitivity classification must be upgraded so that its classification reflects the highest sensitivity

classification. For example, if information labeled Secret was to be placed on a backup disk containing information with no label (which is by default Internal Use Only), then the backup disk must immediately be reclassified as Secret. Likewise, if information with several different data classification levels is resident on a single computer, then the system controls must reflect the requirements associated with most restrictive data classification. In general, because it increases handling costs as well as operational complexity, commingling of information with different sensitivity classifications is discouraged.

4.4.4 Additional Public Information Labels

Unless it is unquestionably already public information (such as a printed marketing brochure), all CDF Board information with a public label must also be labeled "Approved For Public Release" along with the date when the owner declared the information public.

4.4.5 Dictation Machines and Tape Recorders

To reduce the chance of unauthorized disclosure, in general, Employees should not record sensitive information with dictation machines, tape recorders, or similar devices. If the use of these devices is an operational necessity, the proper sensitivity classification must be specified at the beginning and end of each segment of sensitive information. In this case, the recording media must also be marked with the most stringent data classification found on the media. In addition, the media must be protected in accordance with the most stringent classification found on the media, and erased as soon as possible.

4.5 Third Party Interactions

4.5.1 Third Parties and the Need to Know

Unless it has specifically been designated as public, all CDF Board internal information must be protected from disclosure to third parties. Third parties may be given access to the internal information only when a demonstrable need-to-know exists, and when such a disclosure has been expressly authorized by the relevant information owner.

4.5.2 Disclosures to Third Parties and Non-Disclosure Agreements

The disclosure of sensitive information to consultants, contractors, auditors, temporaries, or any other third parties must always be preceded by the receipt of a signed CDF Board non-disclosure agreement (NDA). Disclosures of sensitive information to these third parties must be accompanied by a running log indicating exactly what type of information was provided. This log will be important when the time arrives to recover these materials (or obtain a letter certifying the destruction of the materials) at the end of a contract.

4.5.3 Disclosures from Third Parties and Non-Disclosure Agreements

Employees must not sign non-disclosure agreements provided by third parties without the advance authorization by the legal department as these forms may contain terms and conditions which unduly restrict future business directions.

4.5.4 Prior Review

Every speech, presentation, technical paper, book, or other communication to be delivered to the public must first have been approved for release by the involved employee's immediate manager. This policy applies if the employee will represent CDF Board, if the employee will discuss any affairs (even if only generally), or if the communication is based on information obtained in the course of performing job duties. If research results, corporate strategies, sensitive information, are to be divulged, prior approval of the CEO must to be obtained.

4.5.5 Owner Notification

If sensitive information is lost, is disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, the information owner and the Information Security Team Leader must both be notified immediately.

4.6 Handling

4.6.1 Unattended Printing

Printers must not be left unattended if sensitive information is being printed or will soon be printed. The persons attending the printer must be authorized to examine the information being printed. Unattended printing of sensitive information is permitted only if physical access controls are used to prevent unauthorized persons from both entering the area around the printer and viewing the material being printed.

5.0 E-MAIL SECURITY POLICY

5.1 CDF Board Property

As a productivity enhancement tool, CDF Board encourages the use of electronic communications systems for business purpose notably electronic mail, and fax. Unless third parties have clearly noted, all messages generated on or handled by these systems are considered to be the property of the CDF Board.

5.2 Authorized Usage

CDF Board electronic communications systems generally must be used only for business activities. Incidental personal use is permissible so long as

- It does not consume more than a trivial amount of system resources.
- It does not interfere with worker productivity.
- It does not preempt any business activity.

The electronic communication systems are not to be used for charitable fundraising campaigns, political advocacy efforts, private business activities, or personal amusement and entertainment. Employees are reminded that the use of CDF Board information system resources should never create either the appearance or the reality of inappropriate use.

5.3 Default Privileges

Electronic communication systems must be established and maintained such that only the privileges necessary to perform a job are granted to a worker. This approach is widely known as the concept of "least privilege." When a worker's relationship with CDF Board comes to an end, that entire worker's privileges on the electronic communications systems will also come to an immediate end, i.e. electronic mail will not be forwarded or voice-mail will not be stored.

5.4 User Separation

Electronic mail systems must employ personal user-IDs and associated passwords to isolate the communications of different users.

5.5 User Accountability

Individual passwords must never be shared or revealed to anyone else besides the authorized user. ICT department staff has all the privileges they need in order to do their jobs and therefore, they should never ask users to reveal their passwords. If users need to share computer

resident data, they should utilize message forwarding facilities, public directories on local area network servers, group-databases, and other authorized information-sharing mechanisms.

5.6 User Identity

Misrepresenting, obscuring, suppressing, or replacing another user's identity on an electronic communications system is forbidden. Employees must not send anonymous electronic communications. The user name, electronic mail address, organizational affiliation, and related information included with electronic messages must reflect the actual originator of the messages. At a minimum, all Employees must provide their name, phone, job title, company affiliation, address, and other particulars in all electronic communications.

5.7 Use Only CDF Board Electronic Mail Systems

Unless permission from the Head of ICT has been obtained, employees must not use their personal electronic mail accounts with an Internet Service Provider (ISP) or any other third party for any CDF Board business. Likewise, Employees must not use the electronic mail features found in web browsers for any CDF Board business communications; but must instead employ authorized electronic mail software.

5.8 Respecting Privacy Rights

Employees should not intercept or disclose, or assist in intercepting or disclosing an electronic communications. CDF Board respects the rights of its Employees and also is responsible for operating, maintaining, and protecting its electronic communications networks. However CDF Board may be compelled to employ content monitoring systems.

5.9 No Guaranteed Message Privacy

CDF Board will endeavor to provide all controls necessary to protect the message. However this cannot be guaranteed 100% and Employees should be aware that electronic communications can be forwarded, intercepted, printed, and stored by others. Electronic communications may be accessed by people other than the intended recipients.

5.10 Contents of Messages

Employees must not use profanity, obscenities, or derogatory remarks in electronic mail messages discussing employees, or others, which may create legal problems such as libel and defamation of character.

5.11 Statistical Data

Consistent with generally accepted business practice, CDF Board collects statistical data about its electronic communication systems. ICT personnel monitor the use of electronic communications to ensure the ongoing availability and reliability of these systems. CDF Board employs computer systems, which analyze these types of statistical information to detect unauthorized usage, fraud and other problems.

5.12 Handling Attachments

Attachments to electronic mail messages, if they have any executable code embedded in them, may contain a virus or may in some other way damage a worker's computer. All attachment files should be scanned with an authorized virus detection software package before opening and/or execution. Employees should not open any attachments from unknown senders without getting approval or confirmation of the safety of the attachment from the ICT department.

5.14 Message Forwarding

Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages.

5.15 Handling Alerts about Security

Users must promptly report all information security alerts, warnings, vulnerabilities, and the like to the Information Security/ IT Department. Many of these notices are hoaxes and cause Employees to be distracted from their work. The Information Security Team / ICT department are the only units authorized to determine appropriate action in response to such notices.

5.16 Public Representations

No media advertisement, web-site pages, electronic bulletin board posting, electronic mail message, voice mail message, or any other public representation about CDF Board may be issued unless it has first been approved by the CEO. Likewise, CDF Board as a matter of policy does not send unsolicited electronic mail "spam", nor does it issue unsolicited fax advertising. If Employees are bothered by an excessive amount of spam from a particular organization or electronic mail address, they must not respond directly to the sender. Instead, they must forward samples of the messages to the ICT department who will then take the matter up with the sender's Internet Service Provider (ISP). Employees are also prohibited from "mail bombing" other users in retaliation for any perceived wrong which involves sending a large number of message in order to overload a server or user's electronic mailbox.

5.17 User Back-Up

If an electronic mail message contains information relevant to the completion of a business transaction, contains potentially important reference information, or has value, it should be retained for future reference. Users must regularly move important information from electronic mail message files to word processing documents, databases, and other files. Important old electronic mail messages can be periodically expunged by systems administrators, mistakenly erased by users, and otherwise lost when system problems occur.

5.18 Purging Electronic Messages

Messages no longer needed for business purposes must be periodically purged by users from their personal electronic message storage areas. After six months, e-mail messages stored on CDF Board mail server will be automatically deleted by ICT department staff to increase storage space and also simplify records management and related activities.

5.19 Harassing or Offensive Materials

CDF Board computer and communications systems are not to be used as an open forum to discuss CDF Board organizational changes or business policy matters. This may cause for disciplinary action up to and including termination. Users who receive offensive unsolicited material from outside sources must not forward/redistribute it to either internal or external parties (unless this forwarding/redistribution is to the CDF Board Human Resources Department in order to assist with the investigation of a complaint).

Employees are encouraged to respond directly to the originator of offensive electronic mail messages, telephone calls, and/or other electronic communications. If the originator does not promptly stop sending offensive messages, Employees must report the communications to their manager and the Human Resources Department.

5.20 Paper Confirmation for Contracts

All contracts formed through electronic offer and acceptance messages (fax, electronic data interchange (EDI), electronic mail, etc.) must be formalized and confirmed via paper documents within two weeks of acceptance. Separately, because it could facilitate identity theft and other types of fraud, Employees must not employ scanned versions of hand-rendered signatures to give the impression that an electronic mail message or other electronic communications were signed by the sender.

6.0 FIREWALL POLICY

6.1 Policy Objective and Scope

Firewalls are an essential component of CDF Board's information systems security infrastructure. Firewalls are defined as security systems that control and restrict both Internet connectivity and Internet services. Firewalls establish a perimeter where access controls are enforced. Connectivity, as the word is used here, defines which computer systems can exchange information. A service, as the word is used here, is sometimes called an application, and it refers to the way information is to flow through a firewall. Examples of services include FTP (file transfer protocol) and HTTP (hypertext terminal protocol-web browsing).This policy defines the essential rules regarding the management and maintenance of firewalls at CDF Board and it applies to all firewalls owned, rented, leased, or otherwise controlled by its Employees.

6.2 Playing the Role of Firewalls

In some instances, systems such as routers, air gaps, or gateways may be functioning as though they are firewalls when in fact they are not formally known as firewalls. All systems playing the role of firewalls, whether or not they are called firewalls, must be managed according to the rules defined in this policy. In some instances this will require that these systems be upgraded so that they support the minimum functionality defined in this policy.

6.3 Defined Decision Maker

Before being enabled, all new firewall services and new connectivity paths must be evaluated in terms of business advantages and security risks.

6.4 Default to Denial

Every Internet connectivity path and Internet service not specifically permitted by this policy will be blocked by CDF Board firewalls. The list of currently approved services must be documented and distributed to all systems administrators with a need-to-know by the Information Security Team. Likewise, every network connectivity path not specifically permitted by the Information Security Team must be denied by firewalls. Permission to enable any paths will be granted by the Information Security Team Leader only when:-

1. The paths are necessary for important business reasons.
2. Sufficient security measures will be consistently employed.

6.5 Regular Auditing

Firewalls provide such an important barrier to unauthorized access to CDF Board networks, and such must be audited on a regular basis. At a minimum, this audit process must include consideration of defined configuration parameters, enabled services, permitted connectivity,

current administrative practices, and adequacy of the deployed security measures. These audits must be performed by technically proficient persons other than those responsible for the administration of the involved firewalls.

6.6 Contingency Planning

Technical staff working on firewalls must prepare and obtain Information Security Team Leader approval for contingency plans which address the actions to be taken in the event of various problems including system compromise, system malfunction, system crash, and Internet Service provider (ISP) unavailability. These contingency plans must be kept up-to-date to reflect changes in the CDF Board information systems environment. These plans must also be periodically tested to ensure that they will be effective in restoring a secure and reliable information systems environment.

6.7 External Connections

All in-bound real-time Internet connections to CDF Board internal networks must pass through a firewall before users can reach a login banner. No CDF Board computer system may be attached to the Internet unless it is protected by a firewall. Such computer systems include web servers, electronic commerce servers, and mail servers.

6.8 Firewall Access Mechanisms

All CDF Board firewalls must have unique passwords or other access control mechanisms. The same password or access control code must not be used on more than one firewall. This will prevent an intruder from using the same mechanism to compromise multiple firewalls. In certain high security environments, such as the CDF Board Internet remote access for firewall administrators is prohibited; to prevent intruders from altering firewall configurations and causing other trouble, for these environments, all firewall administration activities must take place in person.

6.9 Firewall Access Privileges

Privileges to modify the functionality, connectivity, and services supported by firewalls must be restricted to a few technically-trained individuals with a business need for these same privileges. These privileges are granted only to employees who are full-time permanent employees of CDF Board (no temporaries, contractors, consultants, or outsourcing personnel). All firewalls must have at least two staff members who are adequately trained to make changes as circumstances require.

6.10 Demilitarized Zones

All E-commerce servers including Internet CDF Board Servers must be protected by firewalls in a demilitarized zone (DMZ). Demilitarized zones are subnets which are protected by a firewall from the Internet, but they have another firewall preventing users of the systems in the DMZ from gaining access to other network-connected outside the DMZ.

6.11 Disclosure of Internal Network Information

The internal system addresses, configurations, and related system design information for CDF Board networked computer systems must be restricted such that both systems and users outside the internal network cannot access this information by splitting DNS (Domain Name Service).

6.12 Secure Back-Up

Current off-line back-up copies of firewall configuration files, connectivity permission files, firewall systems administration procedural documentation files, and related files must be kept

close to the firewall at all times. An alternative to off-line copies involves on-line encrypted versions of these files to keep intruders away and at the same time readily available.

6.13 Firewall Dedicated Functionality

Firewalls must run on dedicated machines which perform no other services (such as acting as a mail server). To reduce the chances of security compromise, firewalls must have only the bare minimum of operating systems software resident and enabled on them.

6.14 Firewall Change Control

Because they support critical information systems activities, firewalls are considered to be production systems. This means that all changes to the software provided by vendors (excluding vendor-provided upgrades and patches) must be tested and approved.

6.15 Posting Updates

Because hackers and other intruders use the latest attack techniques, CDF Board firewalls must be running the latest software to repel these attacks. Where available from the involved vendor, all CDF Board firewalls must subscribe to software maintenance and software update services, which must be installed and run these updates within two business days of receipt.

6.22 Monitoring Vulnerabilities

CDF Board staff members responsible for managing firewalls must subscribe the emergencies advisories e.g. AVERT advisory from McAfee, Kaspersky and other relevant sources providing current information about firewall vulnerabilities. Any vulnerability which appears to affect the CDF Boards' networks and systems must promptly be brought to the attention of the Information Security Team Leader.

6.23 Firewall Physical Security

All firewalls must be located in locked rooms accessible only to those who must have physical access to such firewalls to perform the tasks assigned by management. The placement of firewalls in the open area within a general-purpose data processing center is prohibited.

7.0 INTERNET POLICY

7.1 Opportunities and Risks

The wide array of new resources, new services, and interconnectivity available via the Internet all introduce new business opportunities as well as new security and privacy risks. In response to the risks, this policy describes CDF Board's official policy regarding Internet security.

7.2 Applicability

This policy applies to all Employees (employees, contractors, consultants, temporaries, volunteers, etc.) who use the Internet with CDF Board computing or networking resources. All Internet users are expected to be familiar with and fully comply with this policy. Violations of this policy will lead to revocation of system privileges and/or disciplinary action up to and including termination.

7.3 Prior Management Approval

Access to the Internet (apart from electronic mail) will be provided to only those employees who have a legitimate business need for such access. The ability to surf the web and engage in other Internet activities is not a fringe benefit to which all Employees are entitled.

7.4 Information Reliability

All information taken off the Internet should be considered suspect until confirmed by separate information from another source. There is no quality control process on the Internet, and a considerable amount of its information is outdated, inaccurate and in some instances even deliberately misleading. Accordingly, before using free Internet-supplied information for business decision-making purposes, Employees must corroborate the information by consulting relevant sources.

7.5 Virus Checking

All non-text files (databases, software object code, spreadsheets, formatted word processing package files, etc.) downloaded from non-CDF Board sources via the Internet will be screened with virus detection software prior to being used. Whenever an external provider of the software is not trusted, downloaded software should be tested on a stand-alone non-production machine that has been recently backed-up. Downloaded files must be decrypted and decompressed before being screened for viruses.

7.6 Push Technology

Automatic updating of software or information on CDF Board computers via background "push" Internet technology is prohibited unless the involved vendor's system has first been tested and approved. While it is powerful and useful, this technology could be used to spread viruses, and cause other operational problems such as system unavailability.

7.7 Spoofing Users

Unless tools like digital signatures and digital certificates are employed, it is relatively easy to spoof the identity of another user on the Internet. Before staff release any internal information or order any products via public networks, the identity of the individuals and organizations contacted must be confirmed. Identity confirmation is ideally performed via digital signatures or digital certificates, but in cases where these are not available, other means such as letters of credit, third party references, and telephone conversations may be used.

7.8 User Anonymity

Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or any CDF Board electronic communications system is forbidden. The user name, electronic mail address, Job title and related information included with messages must reflect the actual originator of the messages. If users have a need to employ re-mailers or other anonymous facilities, they must do so on their own time, with their own systems, and with their own Internet Service Provider (ISP) accounts.

7.9 Attachments

Employees must not open electronic mail attachments unless they were expected from a known and trusted sender. Such attachments may include viruses or other malicious software.

7.10 Web Page Changes

Employees will not establish new Internet web pages dealing with CDF Board business, or make modifications to existing web pages dealing with CDF Board business, unless they have first obtained the necessary approval. Modifications include the addition of links to other sites, updating the information displayed, and altering the graphic layout of a page.

7.11 Information Exchange

In keeping with the confidentiality agreements signed by all Employees, CDF Board software, documentation, and all other types of internal information must not be sold or otherwise

transferred to any non-CDF Board party for any purposes other than business purposes expressly authorized by management. Exchanges of software and/or data between CDF Board and any third party will not proceed unless a written agreement has first been signed. Such an agreement must specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected.

7.12 Posting Materials

Employees must not post unencrypted CDF Board material (software, internal memos, policies, etc.) on any publicly-accessible Internet computer which supports anonymous FTP or similar publicly-accessible services, unless the posting of these materials has first been approved by the CEO.

7.13 External Representations

Employees may indicate their affiliation with CDF Board in mailing lists, chat sessions, and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied, for instance via an electronic mail address. In either case, whenever Employees provide an affiliation, unless they have been expressly designated as a spokesperson of CDF Board, they must also clearly indicate the opinions expressed are their own, and not necessarily those of CDF Board.

7.14 Appropriate Behavior

To avoid libel, defamation of character, and other legal problems, whenever any affiliation with CDF Board is included with an Internet message or posting, "flaming" or similar written attacks are strictly prohibited. Likewise, Employees must not make threats against another user or organization over the Internet. All Internet messages intended to harass, annoy, or alarm another person are similarly prohibited.

7.15 Removal of Postings

Those messages sent to Internet discussion groups, electronic bulletin boards, or other public forums, which include an implied or explicit affiliation with CDF Board, may be removed if management deems them to be inconsistent with its business interests or existing CDF Board policy. Messages in this category include:

(a) Political statements,
(b) Religious statements,
(c) Cursing or other foul language, and
(d) Statements viewed as harassing others based on race, creed, color, age, sex, physical handicap, or sexual orientation.

7.16 Disclosing Internal Information

Employees must not publicly disclose internal information via the Internet that may adversely affect CDF Board's public relations and internal information systems problems and the like. Responses to specific Government department electronic mail messages are exempted from this policy.

7.17 Inadvertent Disclosure

Care must be taken to properly structure comments and questions posted to mailing lists, public news groups, UseNet, and related public postings on the Internet. Before posting any material, staff must consider whether the posting could put CDF Board at significant disadvantage or whether the material could cause problems.

7.18 Copyrights

CDF Board strongly supports strict adherence to software vendors' license agreements. Copying of software in a manner that is not consistent with the vendor's license is strictly forbidden. Likewise the participation in pirate software bulletin boards and similar activities represent a conflict of interest with CDF Board work, and are therefore prohibited. Similarly, the reproduction, forwarding, or in any other way republishing or redistribution of words, graphics, or other copyrighted materials must be done only with the permission of the author/owner. Employees should assume that all materials on the Internet are copyrighted unless specific notice states otherwise. When information from the Internet is integrated into internal reports or used for other purposes, all material must include labels such as "copyright, all rights reserved" as well as specifics about the source of the information (author names, URLs, dates, etc.).

7.19 Browser User Authentication

Users must not save passwords in their web browsers or electronic mail clients because this may allow anybody who has physical access to their workstations to access the Internet with their identities, as well as read and send their electronic mail. Instead, passwords must be provided each time that a browser or electronic mail client is invoked. Browser passwords may be saved if and only if a boot password must be provided each time the computer is powered-up, and if a screen saver password must be provided each time the system is inactive for two (2) minutes.

7.20 Internet Service Providers

Employees must not employ Internet Service Provider (ISP) accounts and dial-up lines to access the Internet with CDF Board computers. Instead, all Internet activity must pass through CDF Board firewalls so that access controls and related security mechanisms can be applied. Likewise, users must always employ their CDF Board electronic mail address for Internet electronic mail; use of a personal electronic mail address for this purpose is prohibited.

7.21 Establishing Network Connections

Unless the prior approval of the Head of ICT has been obtained, Employees will not establish Internet or other external network connections that could allow non-CDF Board users to gain access to its systems and information. These connections include the establishment of multi-computer file systems (like Sun's NIS), Internet web pages, Internet commerce systems, FTP servers, Pear to Pear and the like.

7.22 Establishing New Business Channels

Unless the CEO have all approved in advance, Employees are prohibited from using new or existing Internet connections to establish new business channels. These channels include electronic data interchange (EDI) arrangements, electronic malls with on-line shopping, on-line database services, etc.

7.23 Personal Use

CDF Board management encourages Employees who have been granted Internet access to explore the Internet, but if this exploration is for personal purposes, it must be done on personal, not company time. Likewise, games, news groups, and other non-business activities must be performed on personal, not company time. Employees must not employ the Internet or other internal information systems in such a way that the productivity of other Employees is eroded; examples include chain letters and broadcast charitable solicitations.

7.24 Blocking Sites

CDF Board firewalls routinely prevent users from connecting with certain non-business web sites. Employees who discover that they have connected with a web site that contains sexually

explicit, racist, violent, or other potentially offensive material must immediately disconnect from that site. The ability to connect with a specific web site does not in itself imply that users of CDF Board systems are permitted to visit that site.

7.25 Management Review

At any time and without prior notice, the management reserves the right to examine electronic mail messages, files on personal computers, web browser cache files, web browser bookmarks, logs of web sites visited, and other information stored on or passing through CDF Board computers. Such management access assures compliance with internal policies and assists with internal investigations.

7.26 Logging

CDF Board routinely logs web sites visited, files downloaded, time spent on the Internet, and related information. Department managers receive reports of such information and use it to determine what types of Internet usage are appropriate for their department's business activities.

7.27 Junk E-mail

Users are prohibited from using CDF Board computer systems for the transmission of unsolicited bulk e-mail advertisements or commercial messages which are likely to trigger complaints from the recipients. Colloquially known as "Spam," these prohibited messages include a wide variety of unsolicited promotions and solicitations such as chain letters, pyramid schemes, and direct marketing pitches. When Employees receive unwanted and unsolicited e-mail (also known as Spam), they must refrain from responding directly to the sender. Instead, they should forward the message to the Head of ICT who can then take steps to prevent further transmissions.

7.28 Notification Process

If sensitive information is lost, any unauthorized use of CDF Board's information systems has taken place or passwords or other system access control mechanisms are lost, stolen, or disclosed, the Head of ICT must be notified immediately. Because it may indicate a computer virus infection or similar security problem, all unusual systems behavior, such as missing files, frequent system crashes, misrouted messages, and the like must also be immediately reported to the Head of ICT. The specifics of security problems should not be discussed widely but should instead be shared on a need-to-know basis.

7.29 False Security Reports

The Internet has been plagued with hoaxes alleging various security problems. Many of these hoaxes take the form of chain letters which request that the receiving party send the message to other people. Staff in receipt of such information about system vulnerabilities must forward it to the Head of ICT, who will then determine what action is appropriate. Employees must not personally redistribute system vulnerability information.

7.30 Testing Controls

Employees must not "test the doors" (probe) security mechanisms at either CDF Board or other Internet. Likewise, both the possession and the usage of tools for cracking information security are prohibited.

8.0 COMPUTER SECURITY POLICY

8.1 Objectives and Scope

A large portion of CDF Board's business is conducted with computers (PCs, workstations and portable computers). Protection of these devices and the information handled or stored in these systems is essential. To this end, this policy provides information security instructions applicable to all Employees (employees, contractors, consultants, temporaries, etc.) who use CDF Board computers. All computer users are expected to comply with this policy as a condition of continued employment. This policy applies whether computers are stand-alone or connected to a network such as a LAN or the intranet.

8.2 Business Use Only

The computers, electronic media and services provided by CDF Board are primarily for business use to assist employees in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-business purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their business purposes. However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

8.3 Changes to Application Software

CDF Board has a standard list of permissible software packages that users can run on their computers. Employees must not install other software packages or permit automatic software installation routines on computers. However upgrades to authorized software will be downloaded to computers by the ICT personnel. Any unapproved software will be removed without any advance notice to the involved worker.

To prevent computer viruses from being transmitted through the CDF Board's computer system, unauthorized downloading of any unauthorized software is strictly prohibited. Employees should contact the **System Administrator** if they have any questions.

8.4 Changes to Operating System Configurations

At no times are Employees allowed to change operating system configurations, upgrade existing operating systems, or install new operating systems. If such changes are required, they will be performed by ICT personnel.

8.5 Changes to Hardware

Computer equipment supplied by CDF Board must not be altered or added to in any way (e.g., upgraded processor, expanded memory, or extra circuit boards). If such changes are required, they will be performed by ICT personnel.

8.6 Virus Program Installed

All computers must continuously run the current version of virus detection. The current version of this anti-virus package will be automatically downloaded to each computer when the machine is connected to CDF Board's internal network. Employees must not abort/disable this download process. At a minimum, this package must execute whenever external storage media is supplied (for example when a flash disk is inserted).

8.7 Decompression before Checking

Externally supplied flash disks, CD-ROMs, and other removable storage media must not be used unless they have first been checked for viruses. Externally supplied computer-readable files (software programs, databases, word processing documents, spreadsheets, etc.) must be decompressed prior to being subjected to an approved virus checking process. If the files have been encrypted, they must be decrypted before running a virus-checking program. Many virus-checking programs cannot detect viruses in compressed or encrypted files.

8.8 Eradicating Viruses

Because viruses can be complex and sophisticated, Employees must not attempt to eradicate them without expert assistance. If Employees suspect infection by a virus, they must immediately stop using the involved computer, turn-off, disconnect from all networks, and call the ICT department.

8.9 Playing With Viruses

Users must not intentionally write, compile, copy, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer system. Such software may be called a virus, bacteria, worm, or a Trojan horse.

8.10 Archival Copies

All computer software must be copied prior to its initial usage, and such copies must be stored in a safe and secure location. These master copies must not be used for ordinary business activities, but must be reserved for recovery from virus infections, hard disk crashes and other computer problems. Documentation about the licenses for such software must be retained to get technical support and verify the legal validity of the licenses.

8.11 Copyright Protection

CDF Board strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. Making unauthorized copies of licensed and copyrighted software, even if only for "evaluation" purposes, is strictly forbidden.

8.12 Deletion of Old Information

Employees are required to delete information from their computers if it is no longer needed or potentially useful. When deleting any information, Employees should use an overwrite program as opposed to use of an "erase" feature (e.g., “Empty Trash”, “Empty Recycle Bin” putting a document in a trash can icon).

8.13 Destruction of Information

Prior to disposal, defective or damaged flash disks or any backup media / reports containing sensitive information must be destroyed using scissors, shredder or other methods available.

8.14 Documentation for Production Systems

Every user who develops or implements software and/or hardware to be used for CDF Board business activities must document the system in advance of its deployment. Such documentation must be prepared even when standard software--such as a spreadsheet program is employed.

8.15 Equipment Theft

All computer equipment is marked with an asset number, which clearly indicates it is CDF Boards’ property. Physical inventories are used to track the movement of computers and related computer equipment.

8.16 Custodians for Equipment

The user of a computer is the custodian of the equipment. If the equipment is damaged, lost, stolen, borrowed, or is unavailable for normal business activities, the custodian must promptly inform their respective business head. Laptops must not be moved or relocated without the knowledge and approval of the involved department manager.

8.17 Use of Personal Equipment

Employees must not bring their own computers, computer peripherals, or computer software into CDF Board facilities without prior authorization.

8.18 Property Pass

Computers, portable computers and related information systems equipment must not leave CDF Board offices unless accompanied by a gate pass signed by a department manager. Equipment owned by Employees and brought into CDF Board premises must also have a property pass. Guards stationed in all CDF Board buildings will check the contents of briefcases, suitcases, handbags, and other luggage to ensure that all equipment leaving CDF Board offices has an approved property pass.

8.19 Positioning Display Screens

The display screens for all computers used to handle sensitive or valuable data must be positioned such that the information cannot be readily viewed through a window, by persons walking in a hallway, or by persons waiting in reception, queue and related areas. Care should also be taken to position keyboards so that unauthorized persons cannot readily see data input.

8.20 Environmental Considerations

To reduce the damage done by electrical power problems, all computers in CDF Board offices must use surge suppressers. Those computers running production applications must also have uninterruptible power systems (UPSs); the premises must be secure, protected against weather elements and hazards including rain, floods, fire, extreme temperatures, tremors, dust and lightning. Liquids, combustible materials, must be kept away from ICT equipment. Air temperature and humidity must be controlled, and monitored by the ICT Head of department or any person from ICT department.

8.21 Procurement of ICT Equipment and Software

Procurement of all hardware, software, peripherals, and network products shall be guided by procurement laws and regulations and **must** conform to specifications by Head of ICT, Software acquired must anticipate future growth, from manufacturer, authorized resellers , must have warranty and must be approved by the C.E.O.

8.22 Maintenance of ICT Equipment

All ICT equipment must be maintained for efficient and smooth operations at the CDF Board Secretariat and at the Constituencies. A service Level Maintenance Agreement expiry of the warranty; only authorized agents or ICT department personnel who are well trained, will be allowed to provide maintenance, and maintenance contracts for all ICT equipment will be maintained by the head of ICT.

8.23 CDF Boarding of ICT Equipment

All ICT equipment shall have a useful life span whose CDF Boarding will be justified by the head of ICT in writing citing reasons. Below in a tabular form is an example of some of the ICT equipment with their useful life spans.

Equipment	Useful life span in Years
Photocopiers	3
Printers	3
Personal Computers / Laptops	3
Servers	5

8.24 Disposal of ICT Equipment

In disposing of ICT resources, cognizance must be taken of public disposal rules and regulations; avoid or minimize degradation to environment; seek authority to donate any computer equipment marked for disposal, remove data and systems or hard disk drives, comply with manufacturers, suppliers or service providers' terms and conditions of disposal and indicated on Disposal Certificate.

9.0 NETWORK SECURITY POLICY

9.1 Purpose

The purpose of this policy is to establish management direction, procedures, and requirements to ensure the appropriate protection of CDF Board information handled by computer networks.

9.2 Scope

This policy applies to all employees, contractors, consultants, temporaries, and other employees at CDF Board, including those employees affiliated with third parties who access CDF Board computer networks. Throughout this policy, the word "worker" will be used to collectively refer to all such individuals. The policy also applies to all computer and data communication systems owned by and/or administered by CDF Board.

9.3 System Access Control

9.3.1 End-User Passwords

Users must always choose passwords that are difficult-to-guess. This means that passwords must NOT be related to a user's job or personal life. Where systems software facilities are available, users will be prevented from selecting easily guessed passwords and be prevented from reusing previous passwords.

Passwords must not be stored in readable form in batch files, automatic login scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorized persons might discover them.

Passwords must not be written down and left in a place where unauthorized persons might discover them. Beside the initial password assignment and password reset situations, if there is reason to believe that a password has been disclosed to someone other than the authorized user, the password must be immediately changed. All passwords must be immediately changed if they are suspected of being disclosed, or known to have been disclosed to anyone besides the authorized user.

Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions that the other party takes with the disclosed password. If users need to share computer resident data, they should use electronic mail, public directories on local area network servers, and other

mechanisms. This policy does not prevent the use of default passwords--typically used for new user-ID assignment or password reset situations--which are then immediately changed when the user next logs-onto the involved system.

9.3.2 Password System Set-Up

All computers permanently or intermittently connected to networks must have password access controls. Multi-user systems must employ user-IDs and passwords unique to each user, as well as user privilege restriction mechanisms. Network-connected single-user systems must employ hardware or software controls that prevent unauthorized access including a screen saver triggered by two (2) minutes of no keyboard and mouse activity.

Access control to files, applications, databases, computers, networks, and other system resources via shared passwords (also called "group passwords") is prohibited.

Wherever systems software permits, the display and printing of passwords must be masked, suppressed, or otherwise obscured such that unauthorized parties will not be able to observe or subsequently recover them.

Wherever systems software permits, the initial passwords issued to a new user by a Security Administrator must be valid only for the new user's first on-line session. At that time, the user must be forced to choose another password. This same process applies to the resetting of passwords in the event that a user forgets a password.

All vendor-supplied default passwords must be changed before any computer or communications system is used for CDF Board business. This policy applies to passwords associated with end-user user-IDs, as well as passwords associated with System Administrator and other privileged user-IDs.

To prevent password guessing attacks where systems software permits, the number of consecutive attempts to enter an incorrect password must be strictly limited. After three (3) unsuccessful attempts to enter a password, the involved user-ID will be suspended or locked out until reset by a System Administrator.

Whenever system security has been compromised, a trusted version of the operating system and all security-related software must be reloaded from trusted storage media such as CD-ROMs, backup disks, or original source code disks. The involved system(s) must then be rebooted.

9.3.3 Log-In/Log-Off Process

All users must be positively identified prior to being able to use any multi-user computer or communications system resources. Positive identification for internal CDF Board networks involves both a user-ID and a password, both of which are unique to an individual user.

Positive identification for users originating external real-time connections to CDF Board systems or networks via value added networks, private business networks (like the CDF Board extranet), public networks (like the Internet), or any other external communications system must involve extended user authentication techniques.

The login process for network-connected CDF Board computer systems will ask the user to login, providing prompts as needed. Specific information about the organization managing the computer, the computer operating system, the network configuration, or other internal matters

must not be provided until a user has successfully provided both a valid user-ID and a valid password.

If there has been no activity on a computer terminal, workstation, or computer for two (2) minutes, the system will automatically bring up the screen-saver and re-establishment of the session will take place only after the user has provided a valid password.

9.4 System Privileges

9.4.1 Limiting System Access

The computer and communications system privileges of all users, systems, and independently operating programs must be restricted based on the need-to-know. This means that privileges must not be extended unless a legitimate business-oriented need for such privileges exists.

Default user file permissions must not automatically allow anyone on the system to read, write, or execute a file. Although users may reset permissions on a file-by-file basis, such permissive default file permissions are prohibited. Nonetheless, default files permissions granted to limited groups of people who have a genuine need-to-know are allowed.

CDF Board computer and communications systems must restrict access to the computers that users can reach over CDF Board networks. These restrictions can be implemented via routers, gateways, firewalls, and other network components. These restrictions must be used to, for example, control the ability of a user to log-into a certain computer then move from that computer to another.

9.4.2 Process for Granting System Privileges

Requests for new user-Ids and changed privileges must be in writing and approved by the user's business head before a System Administrator fulfills these requests (refer to Appendix II for System Access Form).

Individuals who are not CDF Board employees must not be granted a user-ID or otherwise be given privileges to use CDF Board computers or networks for 90 days or less, except Interns. A written approval of a department head must first be obtained.

Special system privileges—must be restricted to those directly responsible for ICT staff on need by need basis. An exception to this policy can be made only if a business head has approved the exception in writing.

Third party vendors must NOT be given dial-up privileges to CDF Board computers and/or networks unless they have a legitimate business need. These privileges must be enabled only for the time period/functions required to accomplish the approved tasks (such as remote maintenance) on a test environment.

All users wishing to use CDF Board internal networks, or systems are connected to CDF Board internal networks, must sign a compliance statement prior to being issued a user-ID. If a certain user already has a user-ID, a signature must be obtained prior to receiving a renewed user-ID. A signature on this compliance statement indicates the involved user understands and agrees to abide by CDF Board policies and procedures related to computers and networks (including the instructions contained in this document).

9.4.3 Process for Revoking System Access

All user-IDS must automatically have the associated privileges revoked after thirty (30) days of inactivity. Users must not test, or attempt to compromise system security measures. Incidents involving system cracking (hacking), password cracking (guessing), file decryption, bootleg software copying, or similar unauthorized attempts to compromise security measures will be considered serious violations of CDF Board policy.

The system privileges granted to users must be reevaluated by management annually. In response to feedback from management, System Administrators must promptly revoke all privileges no longer needed by users.

Management must promptly report all significant changes in worker duties or employment status to the System Administrators/Head of ICT.

9.4.4. Establishment of Access Paths

Changes to CDF Board internal networks include loading new software, changing network addresses, reconfiguring routers, adding dial-up lines, and the like. With the exception of emergency situations, all changes to CDF Board computer networks must be

(a) Documented in a work order request, and
(b) Approved in advance by the ICT Manager except as explicitly delegated by the ICT department. Emergency changes to CDF Board networks must only be made by persons who are authorized by the ICT department. This process prevents unexpected changes from inadvertently leading to denial of service, unauthorized disclosure of information, and other problems. This process applies not only to "Employees" as defined in the scope section of this policy, but also to vendor personnel.

Employees must NOT establish electronic bulletin boards, local area networks, FTP servers, web servers, modem connections to existing local area networks, or other multi-user systems for communicating information without the specific approval of the Head of ICT. Likewise, new types of real-time connections between two or more in-house computer systems must not be established unless such approval has first been obtained. This policy helps to ensure that all CDF Board systems have the controls needed to protect other network-connected systems. Security requirements for a network-connected system are not just a function of the connected system; they are also a function of all other CDF Board connected systems.

All CDF Board computers that intermittently or continuously connect to an internal or external network must employ password-based access controls. Multi-user computers must employ software which restricts access to the files of each user, which logs the activities of each user, and which has special privileges granted to a System Administrator. Single-user systems must employ access control software approved by the Information Security Team Leader that includes boot control and an automatic screen saver, which is invoked after a two (2) minute period of no keyboard activity. Portable computers and home computers that contain CDF Board information are also covered by this policy, as are network devices such as firewalls, gateways, routers, and bridges.

To stop unauthorized system access and related problems, all inter-processor commands from non-CDF Board locations are prohibited unless a user or process has first properly logged-in and valid authorization obtained from Head of ICT.

Users initiating sessions via dial-up lines connected to CDF Board internal networks and/or multi-user computer systems must pass through an additional access control point (firewall)

before users employing these lines can reach a log-in banner. Although other forms of firewalls are possible, CDF Board now provides such access via dynamic passwords. Unless approved in advance by the Head of ICT, dial-up connections that do not go through approved firewalls in order to reach CDF Board internal-network connected systems are prohibited. This policy applies to Internet inbound calls as well as Electronic Data Interchange (EDI).

9.4.5 Computer Viruses, Worms and Trojan Horses

To assure continued uninterrupted service for computers and networks, all computer users must keep approved virus screening software enabled on their computers. This screening software must be used to scan all software coming from either third parties or other CDF Board departments. This scanning must take place before the new software is executed. Users may not bypass scanning processes that could stop the transmission of computer viruses.

Users are responsible for eradicating viruses from all computer systems under their control whenever viruses have been detected using software installed by ICT department staff. As soon as a virus is detected, the involved user(s) must immediately call the ICT department to assure that no further infection takes place. Any experts needed to eradicate the virus are promptly engaged by calling ICT department.

To assist with the post-virus-infection restoration of computer computing environments, all computer software must be copied prior to its initial usage, and such copies must be centrally stored in a designated place. These master copies must not be used for ordinary business activities, but must be reserved for recovery from computer virus infections, hard disk crashes, and other computer problems.

To prevent problems with viruses, worms, and Trojan horses, CDF Board computers and networks must not run software that comes from sources other than:

(a) Business partners,
(b) Knowledgeable and trusted user groups,
(c) Computer or network vendors, or
(d) Commercial software vendors.

Software down-loaded from electronic bulletin boards, shareware, public domain software, and other software from un-trusted sources must not be used unless it has first been subjected to a rigorous testing regimen approved by the Information Security Team Leader

9.4.6 Data and Program Back-up

To protect CDF Board's information resources from loss or damage, computer users are responsible for backing-up the information on their machines. For multi-user computer and communication systems, a System Administrator is responsible for making periodic back-ups. If requested, the ICT department will install, or provide technical assistance for the installation of back-up hardware and/or software.

All sensitive ("confidential"), valuable, or critical information resident on CDF Board computer systems and networks must be periodically backed-up. User department managers must define which information and which machines are to be backed-up, the frequency of back-up, and the method of back-up based on the following guidelines

(1) If the system supports more than one individual and contains data that is critical to day-to-day operations within CDF Board, then back up is required daily.

(2) If the system is used to support job related functions and contains key data critical to the day-to-day operations of that job, then back up is required weekly.
(3) If the system is primarily used as a personal productivity tool and contains no data that would be classified as job or departmental in nature, then back up is at the discretion of the individual user.

Nothing in the timeframes for periodic back up mentioned immediately above restricts the generation of more frequent back-ups, as will occasionally be required for operational and business reasons.

In cases where backup functionality for Operating Systems and Communication devices is not available a printed copy of the configurations is kept safely and any subsequent changes made. Unless the type of information is specifically listed on CDF Board's Information Retention Schedule (available from the Legal department), information must be retained for as long as necessary. Information listed on the Information Retention Schedule must be retained for the period specified. Other information must be destroyed when no longer needed—generally within five (5) years.

To prevent it from being revealed to or used by unauthorized parties, all CDF Board "confidential" information stored on back-up computer media (magnetic tapes, flash disks, optical disks, etc.) must be encrypted using approved encrypting methods.

9.4.7 Portable Computers

Employees in the possession of portable, laptop, notebook, palmtop, and other transportable computers containing "confidential" CDF Board information must not leave these computers unattended at any time.

To prevent unauthorized disclosure, Employees in the possession of transportable computers containing unencrypted "confidential" CDF Board information must not check these computers in airline luggage systems, with hotel porters, etc. These computers must remain in the possession of the traveler as hand luggage.

Whenever "confidential" information is written to a flash disk, magnetic tape, smart card, or other storage media, the storage media must be suitably marked with the highest relevant sensitivity classification. When not in use, this media must be stored in locked safe, locked furniture, or a similarly secured location

9.4.8 Remote Printing

Printers must not be left unattended if "confidential" information is being printed or will soon be printed. The persons attending the printer must be authorized to examine the information being printed. Unattended printing is permitted if the area surrounding the printer is physically protected such that persons who are not authorized to see the material being printed may not enter.

9.4.9 Privacy

Unless contractual agreements dictate otherwise, messages sent over CDF Board computer and communications systems are the property of CDF Board. To properly protect and manage this property, management reserves the right to examine all data stored in or transmitted by these systems. Since CDF Board's computer and communication systems must be used for business purposes only, Employees should have no expectation of privacy associated with the information they store in or send through these systems.

When providing computer-networking services, CDF Board does not provide default message protection services such as encryption. Accordingly, no responsibility is assumed for the disclosure of information sent over CDF Board's networks, and no assurances are made about the privacy of information handled by CDF Board internal networks. In those instances where session encryption or other special controls are required, it is the user's responsibility to make sure that adequate security precautions have been taken. Nothing in this paragraph should be construed to imply that CDF Board policy does not support the controls dictated by agreements with third parties (such as organizations which have entrusted CDF Board with confidential information).

9.4.10 Logs and other systems security tools

To the extent that systems software permits, computer and communications systems handling sensitive, valuable, or critical CDF Board information will securely log all significant security relevant events. Examples include users switching user-Ids during an on-line session, attempts to guess passwords, attempts to use privileges that have not been authorized, modifications to production application software, modifications to system software, changes to user privileges, and changes to logging subsystems.

During this period, logs will be secured such that they cannot be modified, and such that they can be read only by authorized persons. These logs are important for error correction, security breach recovery, intrusion investigations, and related efforts.

To provide evidence for investigation, prosecution, and disciplinary actions, certain information must be captured whenever it is suspected that computer or network related crime or abuse has taken place. The relevant information must be securely stored off-line until such time as it is determined that CDF Board will not pursue legal action or otherwise use the information. The information to be immediately collected includes the system logs, application audit trails, other indications of the current system states, as well as copies of all potentially involved files.

To allow proper remedial action to be taken in a timely manner, records reflecting security relevant events must be periodically reviewed in a timely manner by computer operations staff, information security staff, or systems administration staff.

Users must be put on notice about the specific acts that constitute computer and network security violations. Users must also be informed that such violations will be logged.

Although System Administrators are not required to promptly load the most recent version of operating systems, they are required to promptly apply all security patches to the operating system that have been released by either

(1) Knowledgeable and trusted user groups,
(2) Well-known systems security authorities e.g. antivirus vendors
(3) The operating system vendor

Only those systems security tools supplied by these sources or by commercial software firms may be used on CDF Board computers and networks.

9.4.11 Handling network security information

From time to time, the Head of ICT will designate individuals to audit compliance with this and other computer and network security policies. At the same time, every worker must

promptly report any suspected network security problem—including intrusions and out-of-compliance situations—to the Head of ICT.

All network or systems software malfunctions must be immediately reported to the ICT department. Ignoring these malfunctions could lead to serious problems such as lost or damaged information as well as unavailable network services.

Information about security measures for CDF Board computer and communication systems is confidential and should not be released to people who are not authorized users of the involved systems unless the permission of the Information Security Team Leader has first been obtained.

9.4.13 Physical security of computer and communication equipment

All CDF Board network equipment must be physically secured with anti-theft devices if located in an open office environment. Additional physical access control may also be used for these devices. For example, local area network servers must be placed in locked cabinets, locked closets, or locked computer rooms. Computer equipment located in open service area (CDF Reception areas) must additionally be secured with anti-theft devices.

Server rooms are restricted to: authorized users, fitted with fire detectors, fire extinguishers or automatic fire suppressing equipment and functional Air conditioners all these equipment must be serviced regularly in accordance with the suppliers guide.

Access to systems development staff offices, telephone wiring closets, computer machine rooms, network switching rooms, and other work areas containing "confidential" information must be physically restricted. Management responsible for the staff working in these areas must consult the Information Security Team to determine the appropriate access control method (receptionists, metal key locks, magnetic card door locks, etc.).

All Employees who must keep "confidential" CDF Board information at their homes in order to do their work must receive lockable furniture for the proper storage of this information. At the time of separation from CDF Board, both the furniture and the information stored therein must be immediately returned.

"Confidential" information must not be downloaded to remote locations—such as reception areas, unless proper physical security and encryption facilities are installed and faithfully observed.

9.4.14 ICT Equipment Insurance

All ICT **Equipment** and sensitive data in use and are resident in CDF Boards computer equipment will always be insured with reputable Insurance companies under all risks, especially laptops which must be carried in locked car boots to conceal their presence while travelling. The insurance policy must be renewed annually.

9.4.15 Exception

The Information Security Team Leader acknowledges that under rare circumstances, certain Employees will need to employ systems that are not compliant with these policies. All such instances must be approved in writing and in advance by the Information Security Manager.

9.4.16 Violations

CDF Board Employees who willingly and deliberately violate this policy will be subject to disciplinary action up to and including termination.

10. DATA BACKUP POLICY

10.1 Background

Data can be destroyed by system malfunction or accidental or intentional means. Adequate backups will allow data to be readily recovered as necessary. The ongoing availability of the data is critical to the operation of the CDF Board. In order to minimize any potential loss or corruption of this data, units responsible for providing and operating administrative applications need to ensure that data is adequately backed up by establishing and following an appropriate system backup procedure.

10.2 Purpose

The purpose of this policy is to define the backup requirements for data to be backed up on a daily basis to minimize the exposure to loss of mission critical data. The data minimal data backup policy stipulates the following:

- Software: All software, whether purchased or created personally, is to be protected by at least one full backup.

- System data: System data are to be backed up with at least one backup per month.

- Application data: All application data are to be protected by means of full daily backups (except for Sundays and public holidays).

- User data: All user data located on the file-servers are to be protected by means of full daily backups (except for Sundays and public holidays).

- Storage: All backup media must be stored in a safe and secure location extraneous to the location of the backed up systems. All backup media must be stored in a fireproof safe. All software full backup and monthly backup media must be stored in an off-site backup archive location.

10.3 Guidelines

10.3.1 Retention

CDF Board has established a hierarchical backup cycle, as follows:

- Daily backups (Monday to Friday) are retained for 2 weeks i.e. M1, T1, W1, T1, F1, M2, T2, W2, T2 and F2.

- Weekly backups are retained for 1 month i.e. W1, W2, W3 and W4.

- Monthly backups are retained for 1 year i.e. Month 1 to Month 12. The monthly backup is generated in multiple copies and each copy stored in distinct archive storage location.

- End of fiscal year and yearly data backup is retained for the long-term and should be generated in multiple copies and each copy stored in a distinct archive storage location.

10.3.1 Media Storage

The backup media should be stored in a fireproof and protected location. In the case of magnetic media they should be in a safe that is shielded from electro-magnetic radiation. For maximum safety the archive media should be stored at a site that is remote from where the backup disks are used.

10.3.2 Personnel-in-Charge

The Team Leader – Data Center will manage the End-of-Day (EOD) team in ensuring that at least one primary person is in charge every week and one substitute. Data backup is a critical security measure thus the relevant persons-in-charge of data backup should be committed in writing to adherence to the specific data backup policy and procedures.

10.3.3 Training

All persons-in-charge of data backup will receive adequate training on the data backup process, data restoration process, media rotation, retention and storage. Regular refresher, motivation campaigns and adherence checking on data backup must be conducted.

10.3.3 Documentation

Documentation is necessary for orderly and efficient data backup and restoration. The person-in-charge of data backup should fully document the following items for each generated data backup:

- Date of data backup
- Type of data backup (incremental, full)
- Number of generations
- Responsibility for data backup
- Extent of data backup (files/directories)
- Data media on which the backup data are stored
- Data backup hardware and software (with version number)
- Data backup parameters (type of data backup etc.)
- Storage location of backup copies

10.3.4 Restoration of Data

The restoration of data using data backups must be tested at irregular intervals, at least after every modification to the data backup procedure. It must at least once be proven that complete data restoration is possible (e.g. all data contained in a server must be installed on an alternative server using substitute reading equipment to the data backup writing equipment). This ensures reliable testing as to whether:

- Data restoration is possible
- The data backup procedure is practicable
- There is sufficient documentation of the data backup, this allowing a substitute to carry out the data restoration of necessary
- The time required for the data restoration meets the availability requirements

10.3.5 ICT Human Resource Development Policy

The human resources aspect of ICT is to ensure that the CDF Board has personnel who are able to:

(a) Provide effective and efficient support in the development and maintenance of ICT;
(b) Use ICT to support efficient and effective service delivery;
(c) Innovate and apply new technology consistent with ICT trends.

10.3.6 Capacity building

The head of ICT will be responsible for the determination of overall ICT training needs and capacity building for CDF Board employee, the CDF Board will provide all employees with ICT skills and capabilities necessary for use of ICT resources.
A skill development programme consistent with the overall and Strategic Plan and Human Resource Development policy will be developed and implemented

*

10.3.5 PART VI – BUSINESS CONTINUITY POLICIES

Major operational disruptions pose a substantial risk to the continued operation of the CDFB. The extent to which the CDF Board incorporates the risk of a major operational disruption in its business continuity plan is dependent upon its risk profile.

(i) The CDF Board shall ensure the implementation of the business continuity plan by periodically conducting a business impact analysis at least once a year.
(ii) An organization risk assessment, risk management and risk monitoring to identify the mission critical activities and potential for major disruptions will also be undertaken. The CDF Board should also provide sufficient human and financial resources to support Business Continuity Management.

10.3.6 Responsibilities of the Board members and Top Management

The responsibility for business continuity management rests with the CDF Board and the senior management who are expected to formulate business continuity policy reviews, procedures and guidelines. All these must be documented and reviewed after every two (2) years.

Board members and senior management shall be responsible for:-

(i) Institutionalizing business Continuity Management Document;
(ii) Defining the roles, responsibilities and authority to act in the event of a major disruption;
(iii) Constituting Business Continuity Management Team consisting of:
(iv) Constituting Crisis Management Team consisting of all heads of critical operation areas;
(v) Accountability for business continuity management in cases of outsourced business continuity function.

10.3.7 Risk Assessment

A risk assessment examines the most urgent business functions identified during business impact analysis. It looks at the probability and impact of a variety of specific threats that could cause a business disruption.

The CDF Board shall undertake a Risk Assessment of its ICT processes every one (1) year.

(i) The BC Management Team shall report on the status of business continuity management to the CDF Board and senior management on a regular basis, highlighting where there are identified gaps. This is through implementation status reports, incident reports, testing results and related plans for strengthening the business continuity plan.

(ii) A risk assessment is at a minimum expected to achieve the following;

a. Identify unacceptable concentration of risk and what are known as 'single points of failure'
b. Identify internal and external threats that could cause a disruption and assess their probability and impact.
c. Prioritize threats within the institution.
d. Provide information for a risk control management strategy and an action plan for risks to be addressed.
e. Mitigation of risks through a documented remedial plan.

(iii) Methods and Techniques

The methods and techniques to be used to provide risk assessment include;

a. Insurance statistics;
b. Published disaster frequency statistics;
c. Scoring systems for impact and probability;
d. Gap analysis; and
e. Stress testing.

10.3.8 Business Impact Analysis

Business impact analysis forms the foundation upon which the business continuity plan is developed. It identifies critical business functions and operations that need to be recovered on a priority basis and establishes appropriate recovery objectives for those operations. It should be completed in advance of a risk assessment in order to identify the urgent functions upon which a risk assessment should be focused.

At a minimum a business impact analysis is expected to;

(i) Provide an understanding of CDF Board most critical objectives, the priority, and the timeframes for resumption of each;
(ii) Provide information about resources requirements over time to enable each business function within the organization achieve continuity or resumption of activity within the established timeframes. It should at a minimum identify;

a. Staff numbers and key skills;
b. Data applications and systems;
c. Facilities including alternative location needs, backup strategy policy and schedule. Vendors/ suppliers of various services;
d. Constraints;
e. Mission Critical Activities (MCA's) or tasks that need to be recorded to ensure continuity of the process and business;
f. Dependencies on people, systems, processes, internal and external parties;
g. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for every MCA or business;
h. Systems impact assessment highlighting;
i. Location;
j. Department unit owners, system information, CDF Boarding Dates;
k. Technical person responsible;
l. Provide a list of recovery options for each business process.

(iii) Methods and techniques

(iv) Generally a combination of all the above methods should provide an adequate source of information from which to base the Business continuity Plan. All relevant information should be stored for reference for at least one year or until the next BIA.
(v) Business Impact Analysis (BIA's) must be signed off by department or functional heads through a formal functional process stipulating that they understand, accept and verify BIA's are correct.

10.3.9 Recovery

(i) The CDF Board shall develop recovery procedures that reflect the risk they represent to the operation of its systems taking into consideration the interdependency of risks
(ii) The CDF Board shall facilitate testing of plans to ensure that crisis and recovery teams are aware of their roles and responsibilities in the event of a disruption.
(iii) In cases where the CDF Board shares or outsources a disaster recovery site, there must be service level agreements or contract in place that clearly outline the terms that govern these arrangements between the parties.
(iv) Recovery solutions must be based on Business Impact Assessment (BIA) information.
(v) The business continuity plan should address staff requirements and relocation to the alternate site in the event of a major disruption. A detailed list of tasks for offsite recovery should be made available to all concerned staff.
(vi) CDF Board business continuity management team should:
   a. Identify those business functions and operations to be recovered on a priority basis and establish recovery procedures.
   b. Establish recovery procedures proportional to the risk they pose to the financial system.
   c. There are measure for the quality of planning, competency of staff and effectiveness of the business continuity plan.
   d. There is organizational awareness of emergency procedures and team members and staffs are familiar with their roles, accountability, responsibilities and authority in response to an incident.
   e. All technological, logistical and administration aspects of the business continuity plan have been tested.
   f. The recovery of infrastructure including command centers and of site work is assured.
   g. The availability and relocation of staff is assessed.
   h. Documentation of testing results for the board members, senior management, and auditors.
   i. An inventory of assets needed for offsite recovery should be generated
   j. The alternate site should be sufficiently equipped with the necessary equipment, data and to maintain critical operation and services for a sufficient time period.

(vii) Methods and techniques

Management should develop a test plan for each BCP testing method used. CDF BOARD should employ various methods of exercising including but not limited to the following;

1. Technical Test
2. Desktop/ Orientation/Walkthroughs
3. Live Runs
4. Simulations
5. Integrated tests for departments that are dependent on each other and also stress testing of recovery facilities.

(viii) Communication

CDF Board should include in its business continuity plans procedures for communicating within CDF Board and with relevant external; parties in the event of major disruptions. The CDF Board shall ensure that the response to a disruption is communicated internally and externally to

applicable parties. External communication to the media must only be through external communications teams and approved by senior management or the CDF Board.

(ix) The communication procedures should:

a. Ensure the there is a clear plan identifying staff, for communicating internally (within the organization) and externally (to the public) stakeholders.
b. Establish communication protocols clearly outlining the chain of command from the CDF Board members and Senior Management.
c. Develop a directory for all recovery team members including the crisis management and the emergency management teams, local emergency response organizations and critical service providers.
d. Ensure that the directory/ contact list are made available to all the team members.
e. Address obstacles that may arise due to failure in primary communications systems (electricity, mobile phone network, road network). Ensure that the institution has set up alternative modes of communication.
f. Ensure that copies of business continuity plans are disseminated to the relative personnel.

Approving Executive Name: and Job Title

Approval Date:

Policy Reference Number:

11. APPENDIX

Appendix I – Technology Resource Use Policy