CAREDIRECT

Organization of information security

Version 4.0

2021

Organization’s Internal Data Security Procedures, Actions and Roles.
[<u>CONFIDENTIAL DOCUMENT</u>]

Care Direct SA

Table of Contents

INFORMATION SECURITY IN CAREDIRECT

Information Security Policy

The protection of information systems is of strategic importance for the company in order to achieve its short-term and long-term goals and at the same time, to ensure the privacy of the customers who receive its services.

Care Direct, recognizing the criticality of information systems in the execution of its business functions, implements an Information Security Policy with the aim of:

- Ensuring the confidentiality, integrity, and availability of the information it manages.
- Ensuring the proper operation of information systems.
- The timely response to incidents that may affects the company's business operations.
- Satisfaction of legislative and regulatory requirements.
- The continuous improvement of the level of Information Security.

For that reason:

- The organizational structures that are necessary for the monitoring of issues related to Information Security are defined.
- The technical measures for controlling and restricting access to information and information systems are defined.
- The way of classifying the information according to its importance and value is determined.
- The necessary actions to protect information during the stages of processing, store and distribution, are described.
- The ways of informing and training the employees and associates of the company in matters of Information Security are determined.
- The ways of dealing with Information Security incidents are determined.
- Describes the ways in which the business continuity of the company's operations is ensured in cases of malfunction of information systems or in cases of disasters.

Care Direct makes assessments of the risks associated with Information Security at regular intervals and takes the necessary measures to address them. Implements a framework for evaluating the effectiveness of Information Security procedures through which performance indicators are defined, their measurement methodology is described, and periodic reports are produced which are reviewed by the Management in order to continuously improve the system.

The Information Security Officer has the responsibility to control and monitor the policies and procedures related to Information Security and to take the necessary initiatives to eliminate all those factors that may affect the availability, integrity, and confidentiality of its information.

All employees of Care Direct and its associates with access to information systems of the company, are responsible for complying with the rules of the applicable Information Security Policy.

Management commitment to information security

The **Board of Directors ("the Board")** is ultimately accountable for corporate governance as a whole. The management and control of information security risks is an integral part of corporate governance. In practice, however, the Board explicitly delegates executive responsibilities for most governance matters to the Executive Directors, led by the **Chief Executive Officer (CEO)**.

The **Executive Directors** give overall strategic direction by approving and mandating the information security principles and axioms but delegate operational responsibilities for physical and information security to the **Security Committee (SC)** chaired by the **Chief Security Officer (CSO)**.

The Executive Directors depend heavily on the SC to coordinate activities throughout CARE DIRECT, ensuring that suitable policies are in place to support CARE DIRECT's security principles and axioms. The Executive Directors also rely on feedback from the SC, CSO, ISM, auditors, Risk Management, Compliance, Legal and other functions to ensure that the principles, axioms and policies are being complied-with in practice.

The Executive Directors demonstrate their commitment to information security by:

- A statement of support from the CEO;
- Reviewing and re-approving the principles and axioms every year;
- Approving the IT budget including a specific element set aside for information security;
- Receiving and acting appropriately on management reports concerning information security performance metrics, security incidents, investment requests *etc*.

Information security co-ordination

Information security activities should be co-ordinated throughout CARE DIRECT to ensure consistent application of the security principles, axioms and policy statements.

The Executive Directors have charged the SC with the task of securing CARE DIRECT's assets. The SC is responsible for:

- Management oversight and direction for both physical and logical aspects of security, including information security;
- Coordinating and directing CARE DIRECT's entire security framework, including the information security controls at all CARE DIRECT locations mediated through the Local Security Committees (see below) ;
- Commissioning or preparing information security policy statements, ensuring their compliance with the principles and axioms approved by the Executive Directors, and formally approving them for use throughout CARE DIRECT;

- Periodically reviewing the security policy statements to ensure the efficiency and effectiveness of the information security controls infrastructure as a whole, recommending improvements wherever necessary;
- Identifying significant trends and changes to CARE DIRECT's information security risks and, where appropriate, proposing changes to the controls framework and/or policies for example by sponsoring major strategic initiatives to enhance information security;
- Reviewing serious security incidents and, where appropriate, recommending strategic improvements to address any underlying root causes;
- Periodically reporting on the status of the security controls infrastructure to the Executive Directors, and liaising as necessary with the Risk Management and Audit Committees *etc*., using metrics and other information supplied by the CSO, Local Security Committees, the ISM, Internal Audit and others.

The SC delegates some of its responsibilities (for example to the ISM, the Information Security function and Local Security Committees) but remains accountable to the Executive Directors for the overall effectiveness of information security throughout CARE DIRECT.

Business units or locations within CARE DIRECT have **Local Security Committees (LSCs)** which report to the SC. LSCs are responsible for:

- Providing the strategic direction, support and resources necessary to manage all types of local security issues and thus ensure that CARE DIRECT's information assets are appropriately and consistently protected;
- Co-ordinating and sharing information with each other to ensure consistent execution of the information security policy manual across all CARE DIRECT locations;
- Identifying specific **Significant Information Assets**, classifying them and nominating suitable **Information Asset Owners** (IAOs) for them;
- Gathering metrics and other information on the overall effectiveness of information security controls in their remit, and reporting this to the SC.

Allocation of information security responsibilities

The Executive Directors have appointed a **Chief Security Officer (CSO)**.   The **CSO** is responsible for:

- Chairing the SC;
- Taking the lead on information governance as a whole for example by issuing the policy manual and by providing the overall strategic direction, support and review necessary to ensure that information assets are identified and suitably protected throughout CARE DIRECT;
- Appointing and managing the ISM and Information Security Management team.

The **ISM** and **Information Security Management** are responsible for:

- Defining technical and non-technical information security standards, procedures and guidelines;
- Supporting IAOs and managers in the definition and implementation of controls, processes and supporting tools to comply with the policy manual and manage information security risks;
- Reviewing and monitoring compliance with the policy statements and contributing to Internal Audit and Control Self Assessment (CSA) processes;
- Collecting, analyzing and commenting on information security metrics and incidents;

- Supporting IAOs in the investigation and remediation of information security incidents or other policy violations;
- Liaising as necessary with related internal functions such as IT Operations, Risk Management, Compliance and Internal Audit, as well as the CSO, LSCs, SC and external functions such as the Police when appropriate;
- Organizing a security awareness campaign for personnel to enhance the security culture and develop a broad understanding of the requirements of ISO/IEC 27002.

Managers throughout CARE DIRECT are responsible for:

- Day-to-day implementation of the information security policy manual;
- Ensuring that suitable technical, physical and procedural controls are in place in accordance with the manual, and are properly applied and used by all workers. In particular, they should take measures to ensure that workers:
  - → Are informed of their obligations to fulfill relevant corporate policy statements by means of appropriate awareness, training and education activities;
  - → Comply with the policy statements and actively support the associated controls; and
  - → Are monitored to assess their compliance with the policy statements and the correct operation of the associated controls, and reminded of their obligations as appropriate;
- Providing the direction, resources, support, and review necessary to ensure that information assets are appropriately protected within their area of responsibility;
- Informing Information Security Management and/or IAOs of actual or suspected policy violations (information security incidents) affecting their assets; and
- Evaluating compliance with the policy axioms through the regular CSA process and occasional Internal Audits.

Information Asset Owners (IAOs) are managers held accountable for the protection of particular Significant Information Assets by their LSC or the SC. IAOs may delegate information security tasks to managers or other individuals but remain accountable for proper implementation of the tasks. IAOs are responsible for:

- Appropriate classification and protection of the information assets;
- Specifying and funding suitable protective controls;
- Authorizing access to information assets in accordance with the classification and business needs;
- [For new application system developments] Undertaking or commissioning information security risk assessments to ensure that the information security requirements are properly defined and documented during the early stages of development;
- Ensuring timely completion of regular system/data access reviews; and
- Monitoring compliance with protection requirements affecting their assets.

All CARE DIRECT workers (*i.e.* employees on the payroll and others acting in a similar capacity, such as contractors, consultants, student placements *etc*.) are responsible for complying with the principles, axioms and policies in the information security policy manual where relevant to their jobs. They are responsible for maintaining the security of all information entrusted to them. Upon hire, as a condition of employment, each worker undertakes to comply with CARE DIRECT's information security policies. Any worker failing to comply with the security policies could be subject to disciplinary action, potentially including termination of employment or contract and/or prosecution.

Exemptions process: an IAO may propose exemptions to principles, axioms or policy statements identified in the policy manual for an information asset under their remit. The ISM is responsible for analyzing risks arising from the proposed exemptions and, in most cases, specifying mitigating controls to minimize those risks. Proposed exemptions which the ISM considers could significantly impact CARE DIRECT's information security risks may be referred up through the LSC, SC, CSO and/or the Executive Directors for approval, depending on the significance of the perceived risk. A program (action plan) is normally required to ensure full compliance with the within a specified time frame, in other words exemptions are not indefinite. The IAO will be held accountable for the mitigating controls and the action plan, and must personally assume any additional risk relating to the policy exemption and the mitigating controls until the exemption is resolved.

Current exemptions must be reviewed at least annually by the SC, LSCs, CSO and ISM. In an annual status report to the Executive Directors, authorized exemptions must be listed, the reasons why policy exemptions exist must be clarified and plans to resolve the non-compliance with policy (typically by means of strategic investment to achieve compliance, or by modifying the policy) must be explained.

DATA SECURITY MEASURES

Physical security is the first ring in our layered security approach. Without stringent physical security measures, additional network and data security is marginal at best. That's why we have designed our data center and office facilities to be as secured against unauthorized access, theft, fire and other physical threats.

Here are a few of our key-points of security procedures and specifications, on hardware, software, and data levels, kept by the Call Center.

- IT security personnel (system administrators, network administrators, head of security) use Two Way Authentication through username/password and special access cards in order to have access to critical h/w and s/w systems and/or data.
- Checking, inspection, and supervision of the computers' security by the IT personnel per regular time intervals, through a physical checking of the equipment both on a software and hardware level.
- The agents are trained and informed on security matters like viruses, macro viruses, and the protection of personal data.
- The agents have limited access in the hardware/software parts of the computers, like cd-r, HDs, installing / uninstalling programs, Internet and e-mail. This is affected through usage of the Windows NT's security policy (profiles & system policies), and adjustment of the computer's BIOS.
- Security of computer and telecommunication equipment through usage of an electronic access control system in the Computer Room, as well as through a systematic inventory of hardware and software by the IT department.
- Data export from the system can be affected only by authorized personnel, through usage of official procedures (see Data Extraction Policy).
- Backup of all systems in regular time intervals, in order to have auxiliary data and transaction copies (see document: Database Backup Policy).
- All systems are equipped with anti-virus and firewall applications that are continuously updated automatically.
- The network administrator gives all users passwords. He is the only one can change them. The only exception is the procedure of Extraction List where the passwords are created by IT Security Manger (see Data Extraction Policy). Correct passwords are assured (eight characters minimum, alphanumeric with special characters etc) which are difficult to be guessed by a third attackers using Dictionary attacks or even brute force methods.
- All applications are activated through usage of username/password.
- Network security is affected by using special protection programs, as well as through a daily supervision by the network administrator.

TECHNICAL CALL CENTER INFRASTRUCTURE

For the implementation of the project Care Direct uses its own premises and technical infrastructure, as well as its experienced personnel. More specifically, Care Direct's technological infrastructure comprises of:

Infrastructure Overview

The company is located in three sites. The site referred in this section as 'main', hosts the bulk of our network infrastructure and supports the networks of the two other sites. The Hardware and Network topology is based on the standard needs of the IT industry and we confirm its accuracy and completeness.

Bandwidth

The main site of the company is connected to Internet through a 100 Mbps dedicated connection. The satellite sites are connected with the main site through Sophos RED Devices over Point-to-Point VPN.

Security

The network is protected with the Sophos software firewall. Firewall functions are also provided by the Sophos XG 230 Appliances. Sophos Antivirus protects the network against viruses. Finally, user authentication is enforced by the Domain Controllers.

Backup System

The basic Software that composes the backup system is the StorageCraft, which offers maximum performance, scalability, and reliability. It is connected to the Storage Systems using optical fibers. Also, we sync the backup systems to 20TB Mega Drive on Cloud as Disaster Recovery. This hardware is accompanied by the following software packages:

- Synology NAS DS220+
- Synology NAS DS218+
- StorageCraft for Windows Physical Machine
- StorageCraft for Windows Virtual Machine
- StorageCraft for Linux Physical Machine
- StorageCraft for Linux Virtual Machine

Supportive Systems

A UPS and a generator that reassures the constant 24hour function support all of the systems. The working stations of the agents are equipped with the following equipment:

Internet Access

Every operator has the ability to easily and quickly search for the necessary sites in the Web, and collect all the available information.

PABX – ACD

Care Direct has the switchboard provide by Avaya. The model is Definity G3Si R12 Communication manager 2, Lucent Technology Call center that supports the operation of the call routing system ACD and has a capacity of 8 PRI.

The characteristics of the switchboard are the following:

- Dual calling Direct Dialling In/ Dialling Out for incoming and outbound calls – call routing to designated phones
- Multi level blocking ability based on the use of personal codes, date, time etc
- Abbreviated Dialling
- Hunting Groups
- Hot Lines between users
- Automatic call routing through private or public network based on the most economical route for the specific phone number at the specific day and time
- Night service for inbound calls for answering groups or for the entire call center
- Call routing to different dedicated agent groups
- Last Number Dialled option
- Music- on-hold
- Ability for parallel hearing and intervening during a call by authorized personnel for provision of advice and guidance
- Conference Calling 3 to 6 internal of extract subscribers
- Caller identification with name and phone number indication
- Malicious Call Tracing
- Call Forwarding
- Ability to answer simultaneously several incoming calls (at least 2 analogical and 3 digital
- Redial
- Ability to record data regarding the call such as date, time, call duration etc
- Auto Call-back
- Hold
- Call Pick-up
- Call transfer
- Selection of different ring tones
- Locking of the caller's device with the use of a personal code

CTI Altitude uCI 7.

CTI Altitude uCI 7 offers sophisticated routing capabilities, which are implemented by plan based on predetermined parameters. Call routing can be also implemented for outbound calls. In this case, calls are grouped and routing to selected agents in order to be executed automatically. This is done, in relation to specific algorithms the outcome of which is related to factors like: the type of the campaign, the list size, the quality of the list and is corrected during the campaign's evolution.

There are three options for outbound campaigns:

- Preview - calls made per customer. It is used in small scale hot calling campaigns
- Progressive – calls made to the whole database with an algorithm that does not trigger statistical approaches as to the probability of free agents
- Predictive – calls made to the whole database, with algorithm that does trigger statistical approaches as to the probability of free agents either by using the busy factor indication or with the use of over dial rate. It is aggressive but effective in large-scale campaigns with a large number of agents.

Data Security and stability

Concerns key-points of security procedures and specifications, on hardware, software, and data levels kept by the Care Direct Call Center. These include:

- Checking, inspection, and supervision of the computers' security by the IT personnel on regular time intervals, through a physical checking of the equipment both on a software and hardware level.
- The agents are trained and informed on security matters like viruses, macro viruses, and the protection of personal data.
- The agents have limited access in the hardware/software parts of the computers, like cd-r, HDs, installing / uninstalling programs, Internet and e-mail. This is accomplished with the use of Windows NT's security policy (profiles & system policies) and adjustment of the computer's BIOS.
- Security of computer and telecommunication equipment through usage of an electronic access control system in the Computer Room, as well as through a systematic inventory of hardware and software by the IT department.
- Data export from the system can be affected only by IT personnel, through usage of personal codes on a database level.
- Backup of all systems in regular time intervals, in order to have auxiliary data and transaction copies.
- All systems are equipped with anti-virus program that is continuously updated automatically from the Internet.
- The network administrator gives all passwords and only he can change them. Thus, correct passwords are assured (eight characters minimum, alphanumeric etc) which are difficult to be bypassed by a third party.
- All applications are activated through usage of username/password.
- Network security is guaranteed by the use of protection programs, as well as through a daily supervision by the administrator of the equipment's activities.

Backup

The basic Software that composes the backup system is the StorageCraft, which offers maximum performance, scalability, and reliability. It is connected to the Storage Systems using optical fibers. Also, we sync the backup systems to 20TB Mega Drive on Cloud as Disaster Recovery. This hardware is accompanied by the following software packages:

- Synology NAS DS220+
- Synology NAS DS218+
- StorageCraft for Windows Physical Machine
- StorageCraft for Windows Virtual Machine
- StorageCraft for Linux Physical Machine
- StorageCraft for Linux Virtual Machine

IVR

IVR exploits the CTI platform by adding voice processing machine abilities. The objective is to decrease the time and effort required by customers while at the same time maintaining the quality of the service offered. Meanwhile, through IVR the communication with customers follows a predetermined flow of scenarios regardless of the point where the conversation starts with the customer

IVR presents an innovative and flexible communication tool assisting in:

- Efficient management and exploitation of resources by using IVR to cover a large percentage of easy to answer questions such as FAQ's
- 24X7 coverage including 'difficult' shifts. This parameter is vital for reducing costs and resources required in campaigns where full time service is necessary.

Quality Assurance / Monitoring

In order to maximize the exploitation of the information derived from the communication with the customer, Care Direct uses Avaya's **Bcms Vu** program. It is a reporting accessory for full and detailed statistics. It's use lies only in the gathering of information through time, for example a costumer' s history. With the Bcms Vu the managers of the call center can produce and watch reports that represent information such as:

- Queue behavior
- Performance per agent/ group
- Use/ exploitation of the sources
- Other elements of business performance

Voice Recorder System

Care Direct uses NICE recording system in order to facilitate the quality check procedure of the call center for confirmation / transaction indication, disagreements settlement and the confrontation of legal matters or conventional obligations. With NICE recording system it is possible to print the conversations, record the calls and screen information.

It is an open architecture system that cooperates with different type of systems (call centers, CTI systems) and manufacturers and it provides the user with a friendly interface with easy access to the sound files and the system's management. Furthermore the NICE system provides a united platform on the following Recording possibilities.

- Full Recording: recording of all the calls in cases where recording is a critical control factor of the campaign. NICE records all the inbound and outbound calls and stores them in a database that offers security and the ability for easy search. Different security levels are offered in order to ensure that information won' t be lost.
- Selective Recording: it offers the ability to record partially, for example in specific campaigns or parts of the Service Centers or to choose to record in specific dates and hours. These selective recording algorisms may be random lineal approach or as a percentage.
- Recording on demand **-** it offers members of the responsive team the ability to record the calls whenever they think it is necessary. The selection of the recording is possible during the same time that the call is being carried out.

The NICE system offers the assurance, that all agents fully exploit the Contact's Center applications. Furthermore, NICE can be used to record the agents' and supervisor can monitor and evaluate the agent's performance.
The recorded files can be easily screened using different criteria e.g. the agent that answered the call, the time it was carried out, the duration of the call. The screening can be performed either via an interior phone or via an electronic computer that is placed in the network with a soundboard.
In brief, the system offers the ability to analyze the dialogues and the screens in the time that the user chooses, and offers the ability to organized information storage while maximizing the research speed and placing quality benchmarks.

Reporting

The statistical data are issued in various time periods for a short, medium and long-term assessment and forecast, according to the supervisor's judgment, so as to be able to monitor the call center's performance, to pinpoint problems, and make adjustments.
The reporting applications of the Avaya telephony system: Altitude, Siebel and Voice Recorder record all details regarding outbound calls and therefore can provide information regarding the agents and all call related information (agent id per call, call duration etc). The reporting applications can be customized in order to cover the project's requirements as mentioned in the brief provided by Care Direct.

In addition, Care Direct can provide historical tracking reports on a daily, weekly and monthly basis regarding the:

- Number of outbound calls
- Number of call per type-category-subcategory
- Average call duration
- Number of attempts per record
- Analysis of telecommunication costs (OTE costs)
- Analysis of efficiency per hour per day
- Any additional statistical information requested by Care Direct

BUSINESS CONTINUITY PLAN (BCP)

Introduction

Care Direct S.A. (CD) provide the customer with the best suitable Business Continuity Plan (BCP), which is designed in order for the organization, to prevent, manage, recover and sustain business operations from an emergency, crisis or disaster - and do so promptly, efficiently and economically.

Emergency Concept

Unforeseen or unexpected events causing (e.g.) a failure of information systems over a longer period of time that cannot be tolerated are uniformly designated as emergencies. An emergency causes damage for business operations.

An emergency is always the case if the normal business procedure is disturbed by an event that affects that procedure so negatively as to be intolerable. This is the case if the damage due to the failure significantly exceeds the expenditure for eliminating the cause and its effects.

Basics of BCP

All elements involved are taken into account: physical, IT and human resources, in order to achieve constant communication. For Care Direct the IT plays a pivotal role, and our recovery plan has more focus on systems recovery.

Emergency Management Team

Η Ομάδα Άμεσης Αντίδρασης αποτελεί την πρώτη ομάδα η οποία θα κληθεί σε περίπτωση έκτακτου περιστατικού να εκτιμήσει το μέγεθος των ζημιών και να επαναφέρει σε ομαλή λειτουργία τους χώρους της εταιρείας. Στην ομάδα περιλαμβάνονται και τα άτομα που είναι υπεύθυνα για τα μέσα πυρασφάλειας και την φυσική ασφάλεια των εγκαταστάσεων, με πρωταρχικό σκοπό την αντιμετώπιση πυρκαγιών ή όποιας άλλης κατάστασης εκτάκτου ανάγκης στα πρώτα λεπτά εμφάνισής της.

Ο παρακάτω πίνακας παραθέτει τα στοιχεία των ατόμων που αποτελούν την ομάδα άμεσης αντίδρασης:

Ρόλος	Ευθύνη
CIO/CISO	Team coordination

IT Manager	Information systems status assessment
Land Security Manager	Assessment of the condition of building infrastructure

The responsibilities of the Immediate Response Team include:

- Immediately inform the Management about the situation
- Informing the Response Team
- Safeguarding the safety of staff

Response Team

The Response Team is responsible for coordinating disaster response and restoring systems. Evaluates the extent and impact of the disaster. It is responsible for the IT infrastructure as well as the work of restoring them to normal operation.

The following table lists the details of the individuals who make up the Response Team:

Ρόλος	**Ευθύνη**
CEO	Team coordination
CISO/CIO	Implementation of operational recovery plans
System Admin/s	Implementation of operational recovery plans

The responsibilities of the Response Team are defined hereafter and depending on the severity and type of incident.

Recovery Requirements

Οι χρόνοι επαναφοράς των κρίσιμων λειτουργιών της εταιρείας είναι οι ακόλουθοι:

Activity	MTPD	RTO	RPO	Complete recovery
Development	6 months	48 h	48 h	10 days
Administration	3 months	48 h	7 days	5 days
Premises	1 year	48 h	1 month	3 months
Call Center	6 months	48 h	48 h	10 days

- MTPD (Maximum Tolerable Period of Disruption): the time until the occurrence of unacceptable effects for the company - effects that will jeopardize its viability.
- RTO (Recovery Time Objective): time after the occurrence of the interruption within which the resumption of the activity should be achieved at the required level.
- RPO (Recovery Point Objective): time at which the data of the activity must be recovered, in order for it to be able to return to operation (maximum data loss).
- Full recovery: the time within which full recovery of activity should have been achieved, at the level it was before the outage occurred.

Human Resources

CD invests to 2 persons for the needs of the project. Both persons are very well trained in order to support and fulfil all actions that are expected from the collaboration of CD and CUSTOMER.

The first person will be the main communicator with the CUSTOMER for the needs of the project and will engage 100% of his time to these needs.

In case of his absence (for vacations, illness etc) a second person will undertake his duties until his return.

In case of retirement or resignation of one of the two persons, CD will undertake his/her replacement in a three weeks period, while his/her training will be done "on the job", gradually, using CD's training tools.

In case of a double resignation CD will replace the first position in a three weeks period and the second position in a five weeks period. The training of these persons will be "on the job", gradually, using CD's training tools.

Network – Telecommunications

The communication will be succeeded through different circuits so as to avoid the possibility of non-communication. For example, if there is one malfunctioned circuit, the second circuit will hold the communication and so forth.

In case of a double malfunctioned circuit, CD will restore at least the first circuit in a period of one day. Even though, the restoration of the second circuit will be done in parallel times with the first, it won't exceed the 3 days period.

Through this specific network, CD will undertake all possible queries that concern this collaboration. CD has no obligation to provide any access to its informational systems to CUSTOMER, unless there is a specific need for the specific project. By terminating this need, CD will be cutting off any unauthorized access.

Data Flow

CD is responsible to deliver customer 's data at specific timings. For this purpose CD will provide a well-structured informational system in which all data will be kept in with safety. This system will be supported by the following software and hardware:

- Server
- Operational System
- Data Base
- Back up data system

In case of a malfunction of any of the above, CD will operate will the following ways, according to the problem, in order to restore the problem and ensure the business continuity.

Server

CD's Server is covered by a guarantee. For the whole period of this guarantee, the restoration time is defined from the availability of the spare needed, therefore from the supplier. Usually this time is defined as 15 days from the day of order.

In the case the Server is not covered by any guarantee, the restoration time is again defined from the availability of the spare needed, therefore from the supplier. Usually this time is defined as 30 days from the day of order.

If customer does not agree with above timings, CD and Supplier should sign a specific agreement, causing extra financial demands. For that Customer and CD will need to sign extra agreement.

In the case the specific server cannot be repaired, CD will have to replace it at a maximum of 20 calendar days.

If the problem reflects the data, after replacing the server, CD will have to restore all data at a maximum of 5 calendar days.

Operational System

The system restoration, in the case that doesn't involve the server, will be restored at a period of maximum 3 calendar days.

If the problem involves the data, CD can restore all damaged data at a period of maximum 5 calendar days.

Database

The restoration of Database, if that doesn't involve the above cases, can be done at a period of maximum 7 calendar days.

Access Authorization

Access to the database have only the persons who are involved in the customer's project. There are three levels of security:

- **First level security** (for people who do the data entry in a temporary environment of the database – limited access to the database) or have limited access (Read/Only) to database.
- **Second level security** (for people who run procedures to update the final database from a temporary environment or do updates directly to the database – important access to the database)
- **Third level security** (for administration usage of the database – full access to the database server)

For all the above levels of security username and password is always needed. The authorization of a user is always given from the system administrator and changed periodically. The system administrator updates all security policies with a new user or a user who changes duties or leave the project.

The system administrator has also in duty to check the integrity of the database and report if something abnormal happens.

Call Center

Care Directs´ call center continuity model is designed in order to help the organization to sustain business operations while recovering from disruption - from natural disasters to mere unexpected volume - and do so efficiently, economically, and profitably.

All elements involved are taken into account (physical, IT and human resources) in order to achieve constant communication. For Care Direct the IT plays a pivotal role, and our recovery plan has more focus on systems recovery.

One of the most important ellements of our call center continuity model is to make sure that all of the necessary data is backed up and stored safely offsite. Presently the company is located in three sites. The site referred to in this section as 'main', hosts the bulk of our network infrastructure and supports the networks of the other two sites.

The main site of the company is connected with the Internet through a 512 Kbps dedicated connection. The satellite sites connect with the main site through two dedicated lines 256 Kbps and 512 Kbps respectively.

In each of the two satellite sites there is one Backup Domain Controller. These servers have the following characteristics.

- Siemens Primergy 400
- P4 2.2GHz 254Mb 2x30GB Disk Storage with RAID support.

The basic Software that composes the backup system is the StorageCraft, which offers maximum performance, scalability and reliability. It is connected with the Storage Systems through the use of optical fibers. This hardware is accompanied by the following software packages:

- StorageCraft for Windows Physical Machine
- StorageCraft for Windows Virtual Machine
- StorageCraft for Linux Physical Machine
- StorageCraft for Linux Virtual Machine

The recovery plan also includes a temporary recovery center with 30 fully equipped workstations at: 99, Verginas Str., Ag. Dimitrios, in order to handle live customer calls. At the same time the necessary personnel is fully trained in all recovery procedures.

Care Directs´ call center continuity model is designed in order to help the organization to sustain business operations while recovering from disruption - from natural disasters to mere unexpected volume - and do so efficiently, economically, and profitably.

All elements involved are considered (physical, IT and human resources) in order to achieve constant communication. For Care Direct the IT plays a pivotal role, and our recovery plan has more focus on systems recovery.

One of the most important elements of our call center continuity model is to make sure that all of the necessary data is backed up and stored safely offsite. Presently the company is located in three sites. The site referred to in this section as ‘main’, hosts the bulk of our network infrastructure and supports the networks of the other two sites.

The main site of the company is connected with the Internet through a 512 Kbps dedicated connection. The satellite sites connect with the main site through two dedicated lines 256 Kbps and 512 Kbps respectively.

In each of the two satellite sites there is one Backup Domain Controller. These servers have the following characteristics.

  - Siemens Primergy 400
  - P4 2.2GHz 254Mb 2x30GB Disk Storage with RAID support.

The basic Software that composes the backup system is the StorageCraft, which offers maximum performance, scalability and reliability. It is connected with the Storage Systems through the use of optical fibers. This hardware is accompanied by the following software packages:

- StorageCraft for Windows Physical Machine
- StorageCraft for Windows Virtual Machine
- StorageCraft for Linux Physical Machine
- StorageCraft for Linux Virtual Machine

The recovery plan also includes a temporary recovery center with 30 fully equipped workstations at: 99, Verginas Str., Ag. Dimitrios, in order to handle live customer calls. At the same time the necessary personnel is fully trained in all recovery procedures.

DATABASE BACKUP POLICY

Subject

This procedure describes and explains the necessary steps and controls necessary for the continued efficient and safe archiving of information and database backups.

The ultimate goal is to ensure that:

- A daily backup of the database.
- Keep a copy of the database that ensures continuity and historical data on weekly and monthly level
- A written copy of the remote database to a safe place.

The process is divided into four sections:

1. Daily Back Up. This section refers to the process followed for conducting daily updated copy of the Database and the Archives of the company.
2. Weekly Back Up. This section refers to keeping updated weekly copy of the database and files in a safe place.
3. Monthly Back Up. This section describes the process by which the Care Direct has available at any time up to date copies of the Database and Files in one month period.
4. Annual Back Up. This section describes the process by which the Care Direct has available at any time up to date copies of the Database and Files in one year period.

RESPONSIBILITIES

1. The **Operations Manager** is responsible for taking corrective actions when problems are properly informed and archival copy.
2. The **Network Operator** or the **Database Manager** is responsible for monitoring the continuous updating of copies of the database.
3. The **Account Manager** is responsible for the safe storage of copies of the database in the treasury of the company.
4. The **Operation Manager** or the **Procurement Manager** or an authorized representative shall only have access to safe deposit company.
5. All users in the process are responsible for the smooth implementation of the process.
6. The **Quality Assurance Manager** is responsible for finding over internal controls for detection of implementing this process.

PROCEDURE

Daily Backup.

1. Department of IT: an automatic system has been used so every day at 23:00 the system starts to make Back up all the default files (Database, Data Management Vouchers, Warehouse ERP, records relevant to the operation of the company)
2. Access to server Only: Operations Manager, IT Manager, Network Manager and Officer of the database by passwords kept in a secure file.
3. Each day after the completion of the IT department network administrator or Officer of the Base introduces appropriate magnetic storage media (tapes) on server A (IT) and B (Gravia) to be used for producing copies of the database files. Upon completion of this process complete and sign the appropriate forms. Control Creation Daily copies Base "29-00-01 A" and "29-00-01 B '. Maintained in electronic form.
4. The Network Officer checks the backup results and sign on the electronic form: *Control Creation Daily copies Base «29-00-01 A» and «B 29-00-01."*
5. The daily copies of the database and files stored in the vaults of the Treasury.
6. The Network Manager delivers to Account Manager the Copies of previous day and receives the magnetic materials (tapes) for the next day copy. The daily sheet recycled every week, the same day.

Weekly Backup.

1. On the first working day of each week, Procurement Manager receives weekly copy of the database files from the IT Manager and stores them in a safe place in the company. The weekly copy of recycled every month in the corresponding weekly period of months (the first week, second week, etc.).
2. On receipt of copy of the Base sign on the IT Manager and Supply in Form. Control Creation - Safe Storage Weekly Copy Base "29-00-02". Maintained in electronic form.
3. Access to a safe location within the company have: Operations Manager, Procurement Manager, Chief Accountant, or their representative.

Monthly Backup.

1. On the first working day of each month, the Procurement Officer receives a monthly copy of the database files and stores them in a bank deposit. The monthly copy is recycled each year, apart from the monthly back up of the last months of the year which is not recycled.
2. On receipt of copy of the database IT Manager and Supply Manager sign on a Form: *Safe Storage Weekly Database Copy*.
3. Within the same day, the Supply Manager store copies of the database in the bank.
4. Accesses to Bank have: the Operations Manager, the Supply Manager or their representatives.
5. The IT Manager shall keep records of receipts of updated copies of the database (electronic).
6. At the end of each month (the first business day following) the deposit of the bank are updated copies of the database files for each previous month of the year.

Annual Backup.

1. On the first working day of each year, the Purchasing Manager receives an annual copy of the database files and stores them in the bank deposit. The annual copy of the corresponding monthly copy of the final month of the year, which will be kept for 10 years.
2. On receipt of copy of the Base and signature files on the IT Manager and Supply in the Form. Control Creation - Safe Storage Weekly Copy Base "29-00-02".

REQUIRED DOCUMENTS

- Form. Control Creation Daily copies Base "29-00-01"
- Form. Control Creation - Safe Storage Weekly Copy Base "29-00-02"

DATA EXTRACTION POLICY

This procedure describes and explains the necessary actions by employees of Care Direct for securing and maintaining the company's export files from the bases of Care Direct and its customers in conducting any marketing campaign

RESPONSIBILITIES

- The Database Manager is responsible for the check of the procedure by informing the Operational Director.
- Database Assistant and Database Supervisor are the owners of the exported file.
- Database Manager informs Operational Director for any required changes in the process.
- Operational Director is responsible to check (through audits) that this procedure is applied by all relevant departments and personnel of the company.

PROCEDURE

The process will include the creation of a password by IT Security Manager. The password will only be known by the Database Manager, IT Security Manager and Operational Director and will be used whenever the team requires data extraction.

UPDATE

After entering the password for the extraction, a document will be kept that will contains the following:

- Date & Time version of the extraction file.
- Database from which the extraction was.
- Conditions of the query.
- Customer who requests the extraction.
- Project manager who requests the extraction.
- The Name, signature and position of the employee who made the extraction.
- The Name, signature and position of the person who gave the Password.

EMAIL SECURITY POLICY SUMMARY

This policy defines and distinguished acceptable/appropriate from unacceptable/inappropriate use of electronic mail (email).

Applicability

This is a standard corporate policy that applies throughout the organization as part of the corporate governance framework. It applies to all users of the corporate email systems.

Policy Detail

Background

Email is perhaps the most important means of communication throughout the business world. Messages can be transferred quickly and conveniently across our internal network and globally via the public Internet. However, there are risks associated with conducting business via email. Email is not inherently secure, particularly outside our own internal network. Messages can be intercepted, stored, read, modified and forwarded to anyone, and sometimes go missing. Casual comments may be misinterpreted and lead to contractual or other legal issues.

Policy axioms (guiding principles)

A. Email users are responsible for avoiding practices that could compromise information security.

B. Corporate email services are provided to serve operational and administrative purposes in connection with the business. All emails processed by the corporate IT systems and networks are considered to be the organization's property.

Detailed policy requirements

1. Do not use email:

   - To send confidential/sensitive information, particularly over the Internet, unless it is first encrypted by an encryption system approved by Information Security;
   - To create, send, forward or store emails with messages or attachments that might be illegal or considered offensive by an ordinary member of the public *i.e.* sexually explicit, racist, defamatory, abusive, obscene, derogatory, discriminatory, threatening, harassing or otherwise offensive;
   - To commit the organization to a third party for example through purchase or sales contracts, job offers or price quotations, unless your are explicitly authorized by management to do so (principally staff within Procurement and HR). Do not interfere with or remove the standard corporate email disclaimer automatically appended to outbound emails;
   - For private or charity work unconnected with the organization's legitimate business;

- In ways that could be interpreted as representing or being official public statements on behalf of the organization, *unless* you are a spokesperson explicitly authorized by management to make such statements;
- To send a message from anyone else's account or in their name (including the use of false 'From:' addresses). If authorized by the manager, a secretary may send email on the manager's behalf but should sign the email in their own name *per pro* ('for and on behalf of') the manager;
- To send any disruptive, offensive, unethical, illegal or otherwise inappropriate matter, including offensive comments about race, gender, colour, disability, age, sexual orientation, pornography, terrorism, religious beliefs and practice, political beliefs or national origin, hyperlinks or other references to indecent or patently offensive websites and similar materials, jokes, chain letters, virus warnings and hoaxes, charity requests, viruses or other malicious software;
- For any other illegal, unethical or unauthorized purpose.

2. Apply your professional discretion when using email, for example abiding by the generally accepted rules of email etiquette (see the **Email security guidelines** for more). Review emails carefully before sending, especially formal communications with external parties.
3. Do not unnecessarily disclose potentially sensitive information in "out of office" messages.
4. Emails on the corporate IT systems are automatically scanned for malicious software, spam and unencrypted proprietary or personal information. Unfortunately, the scanning process is not 100% effective (*e.g*. compressed and encrypted attachments may not be fully scanned), therefore undesirable/unsavory emails are sometimes delivered to users. Delete such emails or report them as security incidents to IT Help/Service Desk in the normal way.
5. Except when specifically authorized by management or where necessary for IT system administration purposes, employees must not intercept, divert, modify, delete, save or disclose emails.
6. Limited personal use of the corporate email systems is permitted at the discretion of local management *provided* always that it is incidental and occasional, and does not interfere with business. You should have no expectations of privacy: all emails traversing the corporate systems and networks are subject to automated scanning and may be quarantined and/or reviewed by authorized employees.
7. Do not use Gmail, Hotmail, Yahoo or similar external/third-party email services (commonly known as "webmail") for business purposes. Do not forward or auto-forward corporate email to external/third party email systems. [You may access your own webmail via corporate IT facilities at local management discretion provided that such personal use is strictly limited and is not considered private (see previous statement).]
8. Be reasonable about the number and size of emails you send and save. Periodically clear out your mailbox, deleting old emails that are no longer required and filing messages that need to be kept under appropriate email folders. Send important emails for archival according to the **email archival policy**.

RESPONSIBILITIES

Information Security Management is responsible for maintaining this policy and advising generally on information security controls. Working in conjunction with other corporate functions, it is also responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this policy.

IT Department is responsible for building, configuring, operating and maintaining the corporate email facilities (including anti-spam, anti-malware and other email security controls) in accordance with this policy. In addition it is responsible for assisting users with secure use of email facilities, and acts as a focal point for reporting email security incidents.

All relevant employees are responsible for complying with this and other corporate policies at all times. This policy also applies to third party employees acting in a similar capacity whether they are explicitly bound (*e.g.* by contractual terms and conditions) or implicitly bound (*e.g.* by generally held standards of acceptable behavior) to comply with our information security policies.

Internal Audit is authorized to assess compliance with this and other corporate policies at any time.

INFORMATION SECURITY ON OUTSOURCING

Outsourcing involves transferring responsibility for carrying out an activity (previously carried on internally) to an outsourcer for an agreed charge. The outsourcer provides services to the customer based on a mutually agreed service level, normally defined in a formal contract.

Many commercial benefits have been ascribed to outsourcing, the most common amongst these being:

- Reducing the organization’s costs
- Greater focus on core business by outsourcing non-core functions
- Access to world-class skills and resources

Despite the potential benefits, information security incidents such as inappropriate access to or disclosure of sensitive information, loss of intellectual property protection or the inability of the outsourcer to live up to agreed service levels, would reduce the benefits and could jeopardize the security posture of the organization.

Objective

This policy specifies controls to reduce the information security risks associated with outsourcing.

Scope

The policy applies throughout CARE DIRECT.

Outsourcing providers (also known as outsourcers) include:

- hardware and software support and maintenance staff
- external consultants and contractors
- IT or business process outsourcing firms
- temporary staff

The policy addresses the following controls found in the ISO/IEC 27002:2005 and ISO/IEC 27001 standards:

- 6.2.1 Identification of risks related to external parties
- 6.2.2 Addressing security when dealing with customers
- 6.2.3 Addressing security in third party agreements

Policy axioms

The commercial benefits of outsourcing non-core business functions must be balanced against the commercial and information security risks.

The risks associated with outsourcing must be managed through the imposition of suitable controls, comprising a combination of legal, physical, logical, procedural and managerial controls.

Policy statements

Choosing an outsourcer

Criteria for selecting an outsourcer shall be defined and documented, taking into account the:

- company's reputation and history;
- quality of services provided to other customers;
- number and competence of staff and managers;
- financial stability of the company and commercial record;
- retention rates of the company's employees;
- quality assurance and security management standards currently followed by the company (*e.g*. certified compliance with ISO 9000 and ISO/IEC 27001).

Further information security criteria may be defined as the result of the risk assessment (see next section).

Assessing outsourcing risks

Management shall nominate a suitable CARE DIRECT owner for each business function/process outsourced. The owner, with help from the local Information Risk Management Team, shall assess the risks before the function/process is outsourced, using CARE DIRECT's standard risk assessment processes.

In relation to outsourcing, specifically, the risk assessment shall take due account of the:

a) nature of logical and physical access to CARE DIRECT information assets and facilities required by the outsourcer to fulfill the contract;

b) sensitivity, volume and value of any information assets involved;

c) commercial risks such as the possibility of the outsourcer's business failing completely, or of them failing to meet agreed service levels or providing services to CARE DIRECT's competitors where this might create conflicts of interest; *and*

d) security and commercial controls known to be currently employed by CARE DIRECT and/or by the outsourcer.

The result of the risk assessment shall be presented to management for approval prior to signing the outsourcing contract. Management shall decide if CARE DIRECT will benefit overall by outsourcing the function to the outsourcer, taking into account both the commercial and information security aspects. If the risks involved are high and the commercial benefits are marginal (*e.g*. if the controls necessary to manage the risks are too costly), the function shall not be outsourced.

Contracts and confidentiality agreements

A formal contract between CARE DIRECT and the outsourcer shall exist to protect both parties. The contract shall clearly define the types of information exchanged and the purpose for so doing.

If the information being exchanged is sensitive, a binding confidentiality agreement shall be in place between CARE DIRECT and the outsourcer, whether as part of the outsource contract itself or a separate non-disclosure agreement (which may be required before the main contract is negotiated).

Information shall be classified and controlled in according with CARE DIRECT policy.

Any information received by CARE DIRECT from the outsourcer which is bound by the contract or confidentiality agreement shall be protected by appropriate classification and labeling.

Upon termination of the contract, the confidentiality arrangements shall be revisited to determine whether confidentiality has to be extended beyond the tenure of the contract.

All contracts shall be submitted to the Legal for accurate content, language and presentation.

The contract shall clearly define each party's responsibilities toward the other by defining the parties to the contract, effective date, functions or services being provided (*e.g*. defined service levels), liabilities, limitations on use of sub-contractors and other commercial/legal matters normal to any contract. Depending on the results of the risk assessment, various additional controls should be embedded or referenced within the contract, such as:

- ➢ Legal, regulatory and other third party obligations such as data protection/privacy laws, money laundering *etc*.*;
- ➢ Information security obligations and controls *such as:*
    - o Information security policies, procedures, standards and guidelines, normally within the context of an Information Security Management System such as that defined in ISO/IEC 27001;
    - o Background checks on employees or third parties working on the contract;
    - o Access controls to restrict unauthorized disclosure, modification or destruction of information, including physical and logical access controls, procedures for granting, reviewing, updating and revoking access to systems, data and facilities *etc*.;
    - o Information security incident management procedures including mandatory incident reporting;
    - o Return or destruction of all information assets by the outsourcer after the completion of the outsourced activity or whenever the asset is no longer required to support the outsourced activity;
    - o Copyright, patents and similar protection for any intellectual property shared with the outsourcer or developed in the course of the contract;
    - o Specification, design, development, testing, implementation, configuration, management, maintenance, support and use of security controls within or associated with IT systems, plus source code escrow;
    - o Anti-malware, anti-spam and similar controls;
    - o IT change and configuration management, including vulnerability management, patching and verification of system security controls prior to their connection to production networks;

* In the case of "offshore" outsourcing, special consideration must be given to the ramifications of transferring information between countries or jurisdictions, particularly where privacy and similar laws may conflict. Take qualified legal advice as a matter of course.

- The right of CARE DIRECT to monitor all access to and use of CARE DIRECT facilities, networks, systems *etc*., and to audit the outsourcer's compliance with the contract, or to employ a mutually agreed independent third party auditor for this purpose;
- Business continuity arrangements including crisis and incident management, resilience, backups and IT Disaster Recovery.

Although outsourcers that are certified compliant with ISO/IEC 27001 can be presumed to have an effective Information Security Management System in place, it may still be necessary for CARE DIRECT to verify security controls that are essential to address CARE DIRECT's specific security requirements, typically by auditing them.

Hiring and training of employees

Outsource employees, contractors and consultants working on behalf of CARE DIRECT shall be subjected to background checks equivalent to those performed on CARE DIRECT employees. Such screening shall take into consideration the level of trust and responsibility associated with the position and (where permitted by local laws):

- Proof of the person's identity (*e.g*. passport);
- Proof of their academic qualifications (*e.g*. certificates);
- Proof of their work experience (*e.g*. résumé/CV and references);
- Criminal record check;
- Credit check.

Companies providing contractors/consultants directly to CARE DIRECT or to outsourcers used by CARE DIRECT shall perform at least the same standard of background checks as those indicated above.

Suitable information security awareness, training and education shall be provided to all employees and third parties working on the contract, clarifying their responsibilities relating to CARE DIRECT information security policies, standards, procedures and guidelines (*e.g*. privacy policy, acceptable use policy, procedure for reporting information security incidents *etc*.) and all relevant obligations defined in the contract.

Access controls

In order to prevent unauthorized access to CARE DIRECT's information assets by the outsourcer or sub-contractors, suitable security controls are required as outlined in this section. The details depend on the nature of the information assets and the associated risks, implying the need to assess the risks and design a suitable controls architecture.

Technical access controls shall include:

- User identification and authentication;
- Authorization of access, generally through the assignment of users to defined user roles having appropriate logical access rights and controls;
- Data encryption in accordance with CARE DIRECT's encryption policies and standards defining algorithms, key lengths, key management and escrow *etc*.

- Accounting/audit logging of access checks, plus alarms/alerts for attempted access violations where applicable.

Procedural components of access controls shall be documented within procedures, guidelines and related documents and incorporated into awareness, training and educational activities. This includes:

- Choice of strong passwords;
- Determining and configuring appropriate logical access rights;
- Reviewing and if necessary revising access controls to maintain compliance with requirements;

Physical access controls shall include:

- Layered controls covering perimeter and internal barriers;
- Strongly-constructed facilities;
- Suitable locks with key management procedures;
- Access logging though the use of automated key cards, visitor registers *etc*.;
- Intruder alarms/alerts and response procedures;

If parts of CARE DIRECT's IT infrastructure are to be hosted at a third party data centre, the data centre operator shall ensure that CARE DIRECT's assets are both physically and logically isolated from other systems.

CARE DIRECT shall ensure that all information assets handed over to the outsourcer during the course of the contract (plus any copies made thereafter, including backups and archives) are duly retrieved or destroyed at the appropriate point on or before termination of the contract. In the case of highly classified information assets, this normally requires the use of a schedule or register and a process whereby the outsourcer formally accepts accountability for the assets at the point of hand-over.

Security audits

If CARE DIRECT has outsourced a business function to an outsourcer based at a different location, it shall audit the outsourcer's physical premises periodically for compliance to CARE DIRECT's security policies, ensuring that it meets the requirements defined in the contract.

The audit shall also take into consideration the service levels agreed in the contract, determining whether they have been met consistently and reviewing the controls necessary to correct any discrepancies.

The frequency of audit shall be determined by management on advice from functions such as Internal Audit, Information Security Management and Legal.

Responsibilities

Management

Management is responsible for designating suitable owners of business processes that are outsourced, overseeing the outsourcing activities and ensuring that this policy is followed.

Management is responsible for mandating commercial or security controls to manage the risks arising from outsourcing.

Outsourced business process owners

Designated owners of outsourced business processes are responsible for assessing and managing the commercial and security risks associated with outsourcing, working in conjunction with Information Security, Legal and other functions as necessary.

Information Security

Information Security, in conjunction with functions such as Legal, Compliance and Risk Management, is responsible for assisting outsourced business process owners to analyze the associated risks and develop appropriate process, technical, physical and legal controls. Information Security is also responsible for maintaining this policy.

Internal Audit

Internal Audit is authorized by management to assess compliance with all corporate policies at any time. Internal Audit may assist with audits of outsourcing contracts including security compliance audits, and advise management on the risks and controls relating to outsourcing.

LAPTOP SECURITY POLICY

This policy describes the controls necessary to minimise information security risks affecting CARE DIRECT laptops.

All CARE DIRECT computer systems face information security risks. Laptop computers are an essential business tool but their very portability makes them particularly vulnerable to physical damage or theft. Furthermore, the fact that they are often used outside CARE DIRECT's premises increases the threats from people who do not work for the CARE DIRECT and may not have its interests at heart.

Portable computers are especially vulnerable to physical damage or loss, and theft, either for resale (opportunistic thieves) or for the information they contain (industrial spies).

Do not forget that the impacts of such breaches include not just the replacement value of the hardware but also the value of any CARE DIRECT data on them, or accessible through them. Information is a vital CARE DIRECT asset. We depend very heavily on our computer systems to provide complete and accurate business information when and where we need it. The impacts of unauthorised access to, or modification of, important and/or sensitive CARE DIRECT data can far outweigh the cost of the equipment itself.
This policy refers to certain other/general information security policies, but the specific information given here is directly relevant to laptops and, in case of conflict, takes precedence over other policies.

Physical security controls for laptops

- The physical security of 'your' laptop is your personal responsibility so please take all reasonable precautions. Be sensible and stay alert to the risks.
- Keep your laptop in your possession and within sight whenever possible, just as if it were your wallet, handbag or mobile phone. Be extra careful in public places such as airports, railway stations or restaurants. It takes thieves just a fraction of a second to steal an unattended laptop.
- If you have to leave the PC temporarily unattended in the office, meeting room or hotel room, even for a short while, use a laptop security cable or similar device to attach it firmly to a desk or similar heavy furniture. These locks are not very secure but deter casual thieves.
- Lock the laptop away out of sight when you are not using it, preferably in a strong cupboard, filing cabinet or safe. This applies at home, in the office or in a hotel. **Never** leave a laptop visibly unattended in a vehicle. If absolutely necessary, lock it out of sight in the trunk or glove box but it is generally much safer to take it with you.
- Carry and store the laptop in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage. Don't drop it or knock it about! Bubble-wrap packaging may be useful. An ordinary-looking briefcase is also less likely to attract thieves than an obvious laptop bag.
- Keep a note of the make, model, serial number and the CARE DIRECT asset label of your laptop but do not keep this information with the laptop. If it is lost or stolen, notify the Police immediately and inform the IT Help/Service Desk as soon as practicable (within hours not days, please).

Virus protection of laptops

- Viruses are a major threat to CARE DIRECT and laptops are particularly vulnerable if their anti-virus software is not kept up-to-date. The anti-virus software MUST be updated at least monthly. The easiest way of doing this is simply to log on to the CARE DIRECT network for the automatic update process to run. If you cannot log on for some reason, contact the IT Help/Service Desk for advice on obtaining and installing anti-virus updates.
- Email attachments are now the number one source of computer viruses. Avoid opening any email attachment unless you were expecting to receive it from that person.
- Always virus-scan any files downloaded to your computer from any source (CD/DVD, USB hard disks and memory sticks, network files, email attachments or files from the Internet). Virus scans normally happen automatically but the IT Help/Service Desk can tell you how to initiate manual scans if you wish to be certain.
- Report any security incidents (such as virus infections) promptly to the IT Help/Service Desk in order to minimize the damage
- Respond immediately to any virus warning message on your computer, or if you suspect a virus (*e.g*. by unusual file activity) by contacting the IT Help/Service Desk. Do not forward any files or upload data onto the network if you suspect your PC might be infected.
- Be especially careful to virus-scan your system before you send any files outside the CARE DIRECT. This includes EMAIL attachments and CD-ROMs that you create.

Controls against unauthorized access to laptop data

- **You must use approved encryption software on all corporate laptops, choose a long, strong encryption password/phrase and keep it secure.** Contact the IT Help/Service Desk for further information on laptop encryption. If your laptop is lost or stolen, encryption provides extremely strong protection against unauthorized access to the data.
- You are *personally accountable* for all network and systems access under your user ID, so keep your password absolutely secret. Never share it with anyone, not even members of your family, friends or IT staff.
- Corporate laptops are provided for official use by authorized employees. Do not loan your laptop or allow it to be used by others such as family and friends.
- Avoid leaving your laptop unattended and logged-on. Always shut down, log off or activate a password-protected screensaver before walking away from the machine.

Other controls for laptops

Unauthorized software

Do not download, install or use unauthorised software programs. Unauthorized software could introduce serious security vulnerabilities into the CARE DIRECT networks as well as affecting the working of your laptop. Software packages that permit the computer to be 'remote controlled' (*e.g*. PCanywhere, TeamViewer, etc) and 'hacking tools' (*e.g*. network sniffers and password crackers) are explicitly forbidden on CARE DIRECT equipment unless they have been explicitly pre-authorised by management for legitimate business purposes.

Unlicensed software

Be careful about software licences. Most software, unless it is specifically identified as "freeware" or "public domain software", may only be installed and/or used if the appropriate licence fee has been paid. Shareware or trial packages must be deleted or licensed by the end of the permitted free trial period. Some software is limited to free use by private individuals whereas commercial use requires a license payment. Individuals and companies are being prosecuted for infringing software copyright: do not risk bringing yourself and CARE DIRECT into disrepute by breaking the law.

Backups

Unlike CARE DIRECT servers which are backed up automatically by IT, you must take your own backups of data on your laptop. The simplest way to do this is to logon and upload a data from the laptop to the network on a regular basis – ideally daily but weekly at least. If you are unable to access the network, it is your responsibility to take regular off-line backups to CD/DVD, USB memory sticks *etc*. **Make sure that off-line backups are encrypted and physically secured.** Remember, if the laptop is stolen, lost or damaged, or if it simply malfunctions, it may be impossible to retrieve any of the data from the laptop. Off-line backups will save you a lot of heartache and extra work.

Laws, regulations and policies

You must comply with relevant laws, regulations and policies applying to the use of computers and information. Software licensing has already been mentioned and privacy laws are another example. Various corporate security policies apply to laptops, the data they contain, and network access (including use of the Internet). Visit Information Security's intranet website for further information.

Inappropriate materials

Be sensible! CARE DIRECT will not tolerate inappropriate materials such as pornographic, racist, defamatory or harassing files, pictures, videos or email messages that might cause offence or embarrassment. Never store, use, copy or circulate such material on the laptop and steer clear of dubious websites. IT staff routinely monitor the network and systems for such materials and track use of the Internet: they will report serious/repeated offenders and any illegal materials directly to management, and disciplinary processes will be initiated. If you receive inappropriate material by email or other means, delete it immediately. If you accidentally browse to an offensive website, click 'back' or close the window straight away. If you routinely receive a lot of spam, call IT Help/Service Desk to check your spam settings.

EMAIL SECURITY POLICY

This policy defines and distinguished acceptable/appropriate from unacceptable/inappropriate use of electronic mail (email).

Applicability

This is a standard corporate policy that applies throughout the organization as part of the corporate governance framework. It applies to all users of the corporate email systems.

Policy Detail

Background

Email is perhaps the most important means of communication throughout the business world. Messages can be transferred quickly and conveniently across our internal network and globally via the public Internet. However, there are risks associated with conducting business via email. Email is not inherently secure, particularly outside our own internal network. Messages can be intercepted, stored, read, modified and forwarded to anyone, and sometimes go missing. Casual comments may be misinterpreted and lead to contractual or other legal issues.

Policy axioms (guiding principles)

C. Email users are responsible for avoiding practices that could compromise information security.

D. Corporate email services are provided to serve operational and administrative purposes in connection with the business. All emails processed by the corporate IT systems and networks are considered to be the organization's property.

Detailed policy requirements

9. Do not use email:

   - To send confidential/sensitive information, particularly over the Internet, unless it is first encrypted by an encryption system approved by Information Security;
   - To create, send, forward or store emails with messages or attachments that might be illegal or considered offensive by an ordinary member of the public *i.e.* sexually explicit, racist, defamatory, abusive, obscene, derogatory, discriminatory, threatening, harassing or otherwise offensive;
   - To commit the organization to a third party for example through purchase or sales contracts, job offers or price quotations, unless your are explicitly authorized by management to do so (principally staff within Procurement and HR). Do not interfere with or remove the standard corporate email disclaimer automatically appended to outbound emails;
   - For private or charity work unconnected with the organization's legitimate business;

- In ways that could be interpreted as representing or being official public statements on behalf of the organization, *unless* you are a spokesperson explicitly authorized by management to make such statements;
- To send a message from anyone else's account or in their name (including the use of false 'From:' addresses). If authorized by the manager, a secretary may send email on the manager's behalf but should sign the email in their own name *per pro* ('for and on behalf of') the manager;
- To send any disruptive, offensive, unethical, illegal or otherwise inappropriate matter, including offensive comments about race, gender, colour, disability, age, sexual orientation, pornography, terrorism, religious beliefs and practice, political beliefs or national origin, hyperlinks or other references to indecent or patently offensive websites and similar materials, jokes, chain letters, virus warnings and hoaxes, charity requests, viruses or other malicious software;
- For any other illegal, unethical or unauthorized purpose.

10. Apply your professional discretion when using email, for example abiding by the generally accepted rules of email etiquette (see the **Email security guidelines** for more). Review emails carefully before sending, especially formal communications with external parties.
11. Do not unnecessarily disclose potentially sensitive information in "out of office" messages.
12. Emails on the corporate IT systems are automatically scanned for malicious software, spam and unencrypted proprietary or personal information. Unfortunately, the scanning process is not 100% effective (*e.g*. compressed and encrypted attachments may not be fully scanned), therefore undesirable/unsavory emails are sometimes delivered to users. Delete such emails or report them as security incidents to IT Help/Service Desk in the normal way.
13. Except when specifically authorized by management or where necessary for IT system administration purposes, employees must not intercept, divert, modify, delete, save or disclose emails.
14. Limited personal use of the corporate email systems is permitted at the discretion of local management *provided* always that it is incidental and occasional, and does not interfere with business. You should have no expectations of privacy: all emails traversing the corporate systems and networks are subject to automated scanning and may be quarantined and/or reviewed by authorized employees.
15. Do not use Gmail, Hotmail, Yahoo or similar external/third-party email services (commonly known as "webmail") for business purposes. Do not forward or auto-forward corporate email to external/third party email systems. [You may access your own webmail via corporate IT facilities at local management discretion provided that such personal use is strictly limited and is not considered private (see previous statement).]
16. Be reasonable about the number and size of emails you send and save. Periodically clear out your mailbox, deleting old emails that are no longer required and filing messages that need to be kept under appropriate email folders. Send important emails for archival according to the **email archival policy**.

Responsibilities

- **Information Security Management** is responsible for maintaining this policy and advising generally on information security controls. Working in conjunction with other corporate functions, it is also responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this policy.
- **IT Department** is responsible for building, configuring, operating and maintaining the corporate email facilities (including anti-spam, anti-malware and other email security controls) in accordance with this policy. It is also responsible for assisting users with secure use of email facilities, and acts as a focal point for reporting email security incidents.
- **All relevant employees** are responsible for complying with this and other corporate policies at all times. This policy also applies to third party employees acting in a similar capacity whether they are explicitly bound (*e.g*. by contractual terms and conditions) or implicitly bound (*e.g*. by generally held standards of acceptable behavior) to comply with our information security policies.
- **Internal Audit** is authorized to assess compliance with this and other corporate policies at any time.

Contacts

For further information about this policy or information security in general, contact the Information Security Manager. A variety of standards, procedures, guidelines and other materials supporting and expanding upon this and other information security policies are available in the organization's Information Security Manual, on the corporate intranet and through the Information Security Manager. Local IT/information security contacts throughout the organization can also provide general guidance on the implementation of this policy - contact your line manager or the IT Help/Service Desk for advice.

RISK ASSESMENT POLICY

Purpose

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

Scope

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

Policy

The execution, development and implementation of remediation programs is the joint responsibility of *Information Security Manager* and the department responsible for the systems area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the Security Department Risk Assessment Team in the development of a remediation plan.

Risk Assessment Process

Every specific period of time (usually every 3 months) the Information Security Manager initiates the procedure of penetration test in order to end up with an updated security assessment report. A pre-notice is required to every employee for the time and date of this action will be implemented. In addition, the Information Security Manager is able to perform a penetration test at a random time without pre-notice. The test is using well known penetration testing and vulnerability assessment tools such (but not limited to) as:

- ***Acunetix*** Web Vulnerability Scanner (http://www.acunetix.com/)
- ***Metasploit Framework*** (http://www.metasploit.com/)
- ***Nikto*** Web Scanner (http://www.cirt.net/nikto2)
- ***Nessus*** **–** Internal & External Vulnerability Scanner & Reporting tool (http://www.tenable.com)