



THC RECRUITMENT LTD

Information Security Policy

.....	1
THC RECRUITMENT LTD.....	1
INFORMATION SECURITY POLICY.....	1
PREFACE.....	2
THE RELATIONSHIP BETWEEN POLICIES AND STANDARDS.....	2
INTRODUCTION.....	3
WHAT IS INFORMATION SECURITY?.....	3
SECURITY OF INFORMATION SYSTEMS.....	3
PURPOSE.....	3
COMPLIANCE.....	4
<i>Security Compliance Review</i>	4
<i>Compliance Exceptions</i>	5
<i>Risk Acceptance</i>	5
<i>Approval Process</i>	5
SECURITY POLICY STATEMENTS.....	6
INFORMATION ASSET SECURITY.....	6
ACCESS CONTROL.....	6
<i>Policy Statement</i>	6
PERSONAL USE.....	7
USER IDENTIFICATION AND AUTHENTICATION.....	7
OWNERSHIP RESPONSIBILITIES.....	7
INFORMATION CLASSIFICATION.....	9
SOFTWARE DISTRIBUTION AND LICENSING.....	10
BUSINESS RESUMPTION PLANNING.....	10
BACKUP AND RECOVERY.....	10
PHYSICAL SECURITY OF COMPUTER AND NETWORK RESOURCES.....	11
MINIMUM SECURITY STANDARDS.....	11
PERSONNEL.....	11
PHYSICAL SECURITY.....	11
CONFIDENTIAL WASTE.....	12
END-USER COMPUTING.....	12
SYSTEM INTEGRITY AND ACCESS CONTROL.....	12
PASSWORDS.....	12
COMPUTER OPERATIONS.....	12
NETWORK SECURITY.....	12
DISASTER RECOVERY.....	13
INTERNET USAGE.....	13
MOBILE COMPUTING.....	13
VIRUS CONTROLS.....	13
THIRD PARTY ACCESS.....	13
DIAL-UP CONNECTIONS FOR EXTERNAL TRANSMISSION.....	13

PREFACE

THE RELATIONSHIP BETWEEN POLICIES AND STANDARDS

Having security is a business decision. Attached to any good business decision should be a policy. Security is no different. An information security policy is itself a part of the overall enterprise solution to the security dilemma.

Company Policy communicates management directives which are elaborated more fully in specialised documents such as the IS security policy. A policy is a high level statement of company beliefs, goals, and objectives and the general means for their attainment for a specified subject area.

Information Security Policy contains policies and practices that govern the planning, organization and control of information security. They are management directives that apply to all locations, geographical region or computing platform.

Information Security Standards are a set of best practice criteria for non-specific platforms, applications, technologies and functions. A standard is a mandatory statement of design or implementation. It is also a norm for measurement and, as such, should be restricted to situations where performance to a specific measurement is required.

Specific Implementations includes a set of specific directives for individual platforms, applications, technologies and functions.

INTRODUCTION

What is information security?

The purpose of information security is to ensure business continuity and minimize business damage by preventing or minimizing the impact of security incidents. Information security enables information to be shared, while ensuring the protection of information and computing assets. Information takes many forms. It can be stored on computers, transmitted across networks, printed out or written down on paper. From a security perspective, appropriate protection should be applied to all forms of information, including papers, databases, films, models, tapes, diskettes and any other methods used to convey knowledge and ideas.

Security of Information Systems

Computer systems are powerful tools that touch upon many aspects of life in modern society. They can be used to enhance quality of life or degrade it. The impact of this effect may range from negligible to the dramatic.

To ensure that computer systems are used in an effective and productive way, it is important that the owners, operators and users of these systems have a clear understanding of acceptable standards of use. Such an understanding can be gained as part of an Information Security Policy.

Security of information systems means the protection of the availability, integrity, and confidentiality of information systems. While the growing use of information systems has generated many benefits, it has also shown a widening gap between the need to protect systems and the degree of protection currently in place. All individuals and organizations have a need for proper information system operations. Users must have confidence that information systems will be available and operate as expected without unanticipated failures or problems. Otherwise, the systems and their underlying technologies may not be used to their full potential and further growth and innovation may be prohibited.

Purpose

This document contains senior management policy directives for the security of information throughout THC Recruitment. These directives apply to all THC Recruitment sites, regardless of division, geographical region or computing platform. Individual divisions may have more stringent management requirements.

Responsibility

All personnel who access or make decisions affecting THC Recruitment information play a role in protecting that information. Accordingly, it is expected that all THC Recruitment employees and agents, including but not limited to full-time employees, part-time employees, temporary employees, contractors, vendors and customers that access THC Recruitment systems, will be held personally accountable for protecting THC Recruitment's information.

It is the responsibility of every employee who has knowledge of infringement of these policies to notify his or her department director.

Compliance

Security is very important to the continued health of the business and the maintenance of public trust. While the needs of the business in a particular situation will always determine the appropriateness of any security standard in that situation, non-compliance without valid justification will not be tolerated. All personnel who use, have access to, or are responsible for THC Recruitment information assets must comply with these policies and standards. Violators are subject to disciplinary action, up to and including termination of employment, and legal action.

Security Compliance Review

To ensure observance of the THC Recruitment Information Security Policies, compliance reviews are conducted periodically. These reviews determine whether THC Recruitment information assets are satisfactorily protected. They test the effectiveness of business practice, the safeguards implemented for computer systems, and the security features included in application design plans.

Two organizations are chartered with performing reviews for THC Recruitment information security compliance. They are:

1. I.T. Review

THC Recruitment is responsible for conducting, at a minimum, an annual audit of their respective environment as it relates to the Global Security Policy and for filing a copy of their findings with the Director. This review provides system security consulting and assists in identifying security requirements for THC Recruitment systems.

2. THC Recruitment Internal Auditors

THC Recruitment internal auditors will perform periodic internal control reviews. As part of the evaluation of internal controls over financial systems, internal auditors will evaluate compliance with the THC Recruitment Information Security Policies.

Compliance Exceptions

While the needs of the business may determine the appropriateness of a particular information security policy and/or standard, non-compliance without valid justification is unacceptable. THC Recruitment management may deviate from the THC Recruitment Information Security Policies only when:

1. It has been clearly demonstrated that a cost/benefit analysis of the available compliance options and risk of not complying has been performed,
2. Analysis results indicate that compliance will have a significant and unacceptable business impact.
3. Risk acceptance has been formally approved.

Risk Acceptance

THC Recruitment management must formally accept responsibility for all identified risks when deviating from the THC Recruitment Information Security Policies. Risk acceptances must be:

1. Documented by the Office Manager
2. Approved by the Director

Risk acceptance documentation must include the following information:

- The classification of the information asset(s) at risk.
- A discussion of the compliance options considered and the reason for not complying.
- The risks identified as a result of not complying.
- The estimated cost or operational impact to THC Recruitment if each risk were realized.
- A statement of acknowledgment and acceptance of the identified risks.
- A time period set for periodic review.

Approval Process

Risk acceptances involving information classified as CONFIDENTIAL must be escalated through the following THC Recruitment management levels for approval:

1. The Owner of the information asset in question.
2. The Director to whom the Owner reports (if applicable).

SECURITY POLICY STATEMENTS

INFORMATION ASSET SECURITY

Information is a vital business asset of THC Recruitment. Information, documents, systems, networks, and applications are considered to be information assets. Inadequate protection or misuse of Company information could give competitors an unfair advantage, lessen the quality of THC Recruitment services, instigate legal conflicts, or otherwise harm THC Recruitment.

Policy Statement

It is THC Recruitment policy that all information created, stored, processed, transmitted or printed by or on behalf of THC Recruitment is the property of the Company. This information is an asset of THC Recruitment and all personnel are personally responsible for safeguarding the value, integrity, and confidentiality of Company information assets. All personnel are expected to protect the information assets with which they have been entrusted from unauthorized, deliberate, or accidental:

- Access
- Use
- Modification
- Destruction
- Disclosure
- Possession

ACCESS CONTROL

Policy Statement

It is THC Recruitment policy that access to all information assets must be based strictly on business need (i.e., user access must be restricted to those resources required to perform an authorized job function). Applications, networks, systems, and practices must be designed, developed, configured, and maintained so that users have access to sensitive information and tools only as needed in order to perform their jobs. THC Recruitment services that offer customers or vendors' access to THC Recruitment networks, computer systems, and applications must be designed to maintain the availability, confidentiality and integrity of THC Recruitment information assets.

In order to help achieve this objective, *all new systems* and where deemed necessary, Legacy systems must provide an authenticated user id, access control lists must protect all resources, audit trails must be provided (and themselves protected), and access rights must not be passed to other users to reuse the same items.

Physical access security measures are required to protect against the intentional or accidental intrusion of unauthorized individuals into any area where information assets may be readily accessible.

PERSONAL USE

Policy Statement

The use of THC Recruitment's information assets for unauthorized purposes is not allowed. Using THC Recruitment's computer resources for personal purposes, without supervisory approval is prohibited.

Individuals may not maintain any 'bulletin boards' or other services, which would harm the reputation of the company. Users are specifically prohibited from accessing, downloading, storing, printing or disseminating anything that is considered inappropriate, offensive, illegal, or disrespectful to others.

THC Recruitment also prohibits the conduct of a business enterprise, or of political activity; engaging in any form of organized intelligence collection against THC Recruitment; engaging in fraudulent activities; and knowingly disseminating false or otherwise libellous materials.

All information stored and processed on Company computers and networks is Company property and subject to inspection without notice. Employees should also be aware that suspicious or illegal on-line services are regularly monitored by law enforcement agencies.

USER IDENTIFICATION AND AUTHENTICATION

User identification and authentication is a process to help ensure security of system resources. Identification is determined through the use of a unique user ID. Authentication is the capability to distinguish and verify the identity of an individual.

Policy Statement

It is THC Recruitment policy that all users must be uniquely identified and authenticated before being granted access to information assets. Processes must be established for granting, changing and revoking access to information assets on a timely basis. Such access must be authorized, logged and periodically reviewed. Procedures must specify the process and approvals needed to obtain initial access to information assets, as well as specific actions to be taken when a user leaves the company, changes status or becomes a suspected security risk.

OWNERSHIP RESPONSIBILITIES

All personnel who access or make decisions affecting THC Recruitment information assets play a role in protecting those assets. Business organizations use the concept of ownership to designate decision-making authority for specific information. The owner is that individual business unit director or representative of management who has the responsibility for making and communicating judgments and decisions on behalf of the organization with regard to the use, identification, classification, and protection of a specific information asset. (Note: The ownership role should not be confused with legal ownership. All THC Recruitment information assets are the property of the Company.)

Policy Statement

It is THC Recruitment policy that information asset ownership roles and responsibilities be defined and documented. An owner must be designated for each business critical information asset. For purposes of this statement, the information asset is the logical information/data that is the intellectual property of THC Recruitment.

- Management must formally assign information asset ownership.
- Owners must determine appropriate sensitivity classifications, maximum acceptable unavailability, resource protection and user access requirements. Additionally, owners must implement processes to ensure information assets are appropriately stored, labelled, handled, distributed and used.
- All users of THC Recruitment information assets must comply with all owner-specified control requirements.

Management and employee roles with information security responsibilities include, but are not limited to:

- The Director will have overall custodial responsibility to protect data stored on local corporate computer hardware, responsibility for development of a local Computer Security Plan, and responsibility for development and testing of the corporate business resumption plan. The Director will specify who has ultimate authority to grant access and use corporate computing hardware. In most cases it is assumed that the Director will assign someone to act as his/her designate in the role of Information Security Manager.
- The Director will have direct custodial responsibility for PC's and other computers in their possession that equipment and data, and will be responsible for conformance to the local country or specialty brands detailed computer security plan as it applies.
- The Information Security Manager is responsible for overseeing the administration and distribution of the local computer system security plan. He/She will insure that; the local computer system security plan adheres to the THC Recruitment Security Policy, that reviews are performed as specified, and that only authorized individuals will be allowed access to systems. It is the role of the Information Security Manager to escalate issues as appropriate to the Director. The Information Security Manager will also work with the appropriate personnel to review access controls.
- The Director is responsible for physical security of computer hardware and for availability of computing services as defined in the agreed upon Service Level Agreement Statement. The computer system will be kept within a physically secure area. Only individuals on computer room access list will be given authority and capability to enter the secure area. The Director will maintain the computer room's access list. An authorized individual must escort all other individuals entering the computer room.

- The Director is responsible for integrity of databases that they own, and for defining who shall have read and write access to those databases. They will provide access control methods by which they can secure their data.
- The Office Manager will provide periodic independent appraisals of the computer security controls and techniques with the cooperation of the Director. Continuing and unresolved departures from plan will be reported the Director.
- The Director shall inform the Office Manager of all changing status affecting computer access authority (terminations, promotions, etc.).

INFORMATION CLASSIFICATION

Policy Statement

It is THC Recruitment policy that information assets must be identified, classified, and labelled based on their sensitivity to the organization (i.e., the business impact if destroyed, damaged or disclosed). Owners are responsible for classifying information assets. Everyone is responsible to ensure that the appropriate level of protection is consistently applied.

Classification Categories

Information assets must be classified according to the following scheme:

- **CONFIDENTIAL** - the consequences of disclosure, misuse, or modification of CONFIDENTIAL information could be severe to the Company, its employees, or its customers. CONFIDENTIAL information requires the most stringent access control measures. Examples of CONFIDENTIAL information include marketing plans, customer information, and personnel files.
- **ORGANIZATIONAL** - information that could result in modest financial loss, some increased risk, or some embarrassment to THC Recruitment if disclosed to unauthorized personnel. Material classified as proprietary must be treated with care. Distribution of such materials must be limited to those individuals with a need-to-know. Examples of ORGANIZATIONAL information include organization charts, employee handbooks, and procedure manuals.
- **UNRESTRICTED** - information that can be freely disclosed and used by anyone without limitation. Examples of UNRESTRICTED information include annual financial reports, and product brochures.

Information Labelling

THC Recruitment-approved markings for CONFIDENTIAL and ORGANIZATIONAL information are as follows (information classified as UNRESTRICTED does not require special classification labelling):

- CONFIDENTIAL - “To be used by specific groups of THC Recruitment employees based on job responsibilities or need-to-know.”
- ORGANIZATIONAL - “The information contained herein is for use solely by authorized THC Recruitment employees with a need to know it, and should not be disclosed to others.”

SOFTWARE DISTRIBUTION AND LICENSING

Policy Statement

It is a policy of THC Recruitment that all third-party software used will be properly licensed and terms of the license will be complied with. When at work, or when THC Recruitment computing or networking assets are used, copying of software in a manner not consistent with the vendor’s license is strictly forbidden. Any unlicensed software must be immediately removed from THC Recruitment computers. All software and documentation owned by THC Recruitment must include appropriate copyright notices.

BUSINESS RESUMPTION PLANNING

Policy Statement

It is THC Recruitment policy that information assets be included in local Business Resumption Plans so that business operations will be re-established in the event of a major interruption (e.g., earthquake, flood, fire, civil disruption, etc.). The time frame for re-establishing business operations must be agreed to jointly by the information asset owner and management.

To the extent practical and feasible, Business Resumption Plans must be fully tested at least on an annual basis. A management report is to be prepared which outlines the test results and remedial actions to be taken.

BACKUP AND RECOVERY

Back up of data must be accomplished to protect against loss or corruption of operating systems, systems and application. Critical data/systems must be backed up daily. Backups must be sent to an offsite storage facility in the event that they are required for disaster recovery.

Policy Statement

It is THC Recruitment policy that all CONFIDENTIAL, ORGANIZATIONAL, and UNRESTRICTED information resident on computer systems must be periodically backed-up (business critical files must be backed-up daily) to protect the Company from loss of data due to system failures or file corruption. The Director is responsible for establishing organizational requirements for backups (a backup plan) and for monitoring compliance with their requirements.

THC Recruitment also requires secure on site backup for routine recovery and an archival backup for disaster or long-term recovery. A copy of critical backups must be securely stored offsite.

Certain types of data will need to be backed up more frequently; these decisions must be made on a data-type-by-data-type basis. The specific method to employ for back-ups (grandfather, father, and son rotation for instance) will also be circumstance-dependent. This policy is relevant to microcomputers (PCs), LANs, and client/server systems as well as larger machines.

PHYSICAL SECURITY OF COMPUTER AND NETWORK RESOURCES

Policy Statement

It is THC Recruitment policy that all computer and network resources must be physically secured. Access to every office, computer room, and work area containing sensitive information must be physically restricted.

Minimum Security Standards

The following security standards are a set of best practice information asset protection criteria for non-specific platforms, applications, technologies and functions. Standards and guidelines are rules that must be followed. The topic areas are:

PERSONNEL

Only authorized staff is permitted to use company software and hardware. Company equipment may only be used for official company business.

PHYSICAL SECURITY

Physical access control mechanisms must ensure that access to THC Recruitment office areas not intended for public entry is limited to individuals who can demonstrate their authority to enter. Additionally, Physical access authority must be revoked immediately if the employee's termination is a result of a conflict between the employee and THC Recruitment.

CONFIDENTIAL WASTE

All confidential waste must be appropriately disposed of to ensure that it can not be accessed by any party.

All IT departments operate the Waste Electrical and Electronic Equipment Regulations (EU 2002/96/EC) directive regarding disposal of electrical and electronic equipment, and use a WEEE accredited company to dispose of IT equipment.

END-USER COMPUTING

Commercial software packages provided by the Company should be maintained in locked storage.

SYSTEM INTEGRITY AND ACCESS CONTROL

THC Recruitment must implement a system design that provides for prevention, detection, and recovery from security breaches. Management must provide for recovery in the event that physical destruction, logical destruction, or the corruption of operating systems, software or data occurs. Management must ensure that supporting procedures are in place.

PASSWORDS

A password must be at least 6 characters in length, and must contain numbers and letters. Passwords must be chosen that cannot be easily guessed (e.g. social security number, birth date, family name, car registration, etc.). A user should never give out their password. Requests from individuals for your password whether over the phone or in person are to be refused.

COMPUTER OPERATIONS

Operations and technical support staff must not have access to data, programs, or operating system information beyond that required to perform their jobs.

NETWORK SECURITY

Network documentation will be developed, published, and kept current. The documentation should include schematics of networks and connections, user documentation, system documentation and configuration, problem reporting procedures and contingency plans, and operations documentation.

Access control mechanisms must be able to create an audit trail of accesses to objects (e.g.: Programs, devices, queries, files, etc.) protected by the mechanism. At a minimum, the audit trail will contain all information necessary to trace an individual event back to the point of entry to the local network serving the protected resource.

Special controls (e.g., firewalls) must be established to safeguard systems connected to public (or shared) networks (e.g., the Internet); especially those extending across organizational boundaries to ensure that computer connections and information flow do not breach the access policy of the business applications.

DISASTER RECOVERY

A comprehensive local Business Resumption Plan (BRP) for critical information assets must be developed and regularly updated. Only a complete and up-to-date plan can ensure the continuity and availability of those assets in a crisis. The plan must be regularly tested.

INTERNET USAGE

Non-THC Recruitment External clients or “outsiders” (non-THC Recruitment users) are not permitted access to THC Recruitment’s internal networks unless specifically approved in advance. Under no circumstances should THC Recruitment users establish Internet or other external connections that could allow outsiders to gain access to THC Recruitment’s systems and information. These connections include, but are not limited to, multi-computer file systems, Internet home pages and FTP servers (unless belonging to a technical support company hired by THC Recruitment with advance approval from the Company Director).

MOBILE COMPUTING

Portable computer systems must be secured in locked storage when not in use. Employees using these systems will be responsible for taking all possible measures to protect them when they are not secured.

VIRUS CONTROLS

Computer systems must be equipped with virus protection. Virus detection software must be installed on each microcomputer (PC), workstation or local area network (LAN), and gateways that processes critical or sensitive information. Virus detection software must be run at regular time intervals to scan files for the possible existence of computer viruses. Employees must not attempt to eradicate computer viruses. If they suspect a virus they must immediately stop using the compute and notify the appropriate personnel

THIRD PARTY ACCESS

Access to THC Recruitment information by third parties must be controlled. Where there is a business need for such third party access, a security risk analysis must be carried out to determine the security implications and control requirements. The controls must be agreed and defined in a contract with the third party.

DIAL-UP CONNECTIONS FOR EXTERNAL TRANSMISSION

All dial-up connections for external transmission (e.g., electronic direct deposits to the banks) must be initiated only by authorized THC Recruitment personnel and the modems used for dial-up connection must be set so that they will not answer incoming calls. The dial-up modem phone numbers for the purposes of aforementioned external transmission are considered confidential. Before dial-up connections are turned on, the manager of the department making the connection must make sure that information security standards (e.g., user ID and passwords, etc.) have been followed.