ANNEXURE A: INFORMATION SECURITY LEGISLATION, REGULATIONS AND STANDARDS

1. ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD) SECURITY GUIDELINES

SECURITY LEGISLATION AND REGULATIONS

- 2002 OECD Guidelines for the Security of Information Systems and Networks
- OECD Information Security and Privacy Guidelines
- 1997 OECD Guidelines for Cryptography Policy

2. EUROPEAN UNION SECURITY POLICY DOCUMENTS

2.1 EUROPEAN UNION DIRECTIVES IMPACTING ON INFORMATION SECURITY

- Data Protection Directive (Directive 95/46/EC)
- Electronic Commerce Directive (Directive 2000/31/EC)
- Electronic Signatures Directive (Directive 1999/93/EC)
- Privacy Protection Telecommunication Sector Directive (Directive 97/66/EC)
- Directive on Privacy and Electronic Communications (Directive 2002/58/EC)

2.2 EUROPEAN UNION'S APPROACH TO CYBERCRIME

- Convention on Cybercrime

2.3 EUROPEAN UNION COMMUNICATIONS AND RECOMMENDATIONS

- European Commission Communication: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime
- European Commission Proposal for a Council Framework Decision on Attacks on Information Systems
- Council of Europe resolution on a common approach and specific actions in area of network and information security

3. INTERNATIONAL SECURITY LEGISLATION AND REGULATIONS

CANADA • The Electronic Commerce and Information, Consumer Protection Amendment and Manitoba Evidence Amendment Act (Manitoba Bill C-31) • Information Technology Act (Quebec Bill No. 161)	**UNITED KINGDOM** • Computer Misuse Act 1990 • Data Protection Act 1998 • Telecommunications (Data Protection and Privacy) Regulations 1999 • Freedom of Information Act 2000 • Regulation of Investigatory Powers Act 2000 • Consumer Protection (Distance Selling) Regulation 2000 • Anti-Terrorism, Crime and Security Act 2001 • Electronic Signature Regulation 2002
SOUTH AFRICA • Constitution of South Africa 108 of 1996 • Electronic Communications and Transactions Act 25 of 2002 • Promotion of Access to Information Act 2 of 2000 • Regulation on Interception of Communication-Related Information Act 70 of 2002	**UNITED STATES OF AMERICA** SECURITY LEGISLATION • Homeland Security Act of 2002, H.R. 5005 • USA PATRIOT Act • Security Standard for Health Information (HIPAA) 42 U.S.C. 1320d-2 • Intelligence Authorization Act of 2002 • Federal Information Security Management Act of 2002 (FISMA) CYBERCRIME LAWS • Federal Law Related to Cybercrime • Computer Fraud and Abuse Act of 1986, 18 U.S.C. 1030. • Electronic Communications Privacy Act of 1986 (ECPA) • U.S. Wiretap Law (as amended by ECPA) 18 U.S.C.A. 2510 et al • Store Wire and Electronic Communications Act (18U.S.C. $ 2701-2711) • Electronic Espionage Act of 1996 (18 U.S.C 1831-1839) • Access Code Fraud Act INFORMATION SECURITY AND FEDERAL AGENCIES • Freedom of Information Act 1974 – as amended in 1996 • Privacy Act 1974 • Computer Security Act 1987 • Clinger-Cohen Act 1996 • Paperwork Reduction Act of 1995 • Government Performance and Results Act of 1993 • Federal Acquisition Streamlining Act of 1994 PRIVACY LEGISLATION • Security Standard for Health Information (HIPAA) 42 U.S.C. 1320d-2 • Gramm-Leach-Billey Act (GLB) • Privacy Act 1974 • Freedom of Information Act 1974 – as amended in 1996 • Electronic Communications Privacy Act of 1986 (ECPA) • Computer Security Act 1987 • The Communications Decency Act • Electronic Communications Privacy Act 2000 • Government Information Security Reform Act 2000 • Electronic Signatures in Global and National Commerce Act 2000

(SOURCE: Baker and McKenzie "Global e-commerce law" (last visited 17 September 2003) http://www.bmck.com 1-5).

4. INFORMATION SECURITY STANDARDS AND BEST PRACTICES

- ISO 17799 - International Organisation for Standardisation
- Control Objectives for Information and related Technology (COBIT) - Information Systems Audit and Control Foundation / IT Governance Institute
- Guidelines for the Security of Information Systems and Networks - Organisation for Economic Co-operation and Development (OECD) 2002
- Guidelines for the Management of IT Security - ISO/IEC TR 13335, 1997
- Generally Accepted Systems Security Principles – Pervasive Principles - International Information Security Foundation 1997
- British Standard 7799 – A Code of Practice for Information Security Management, and Specification for Information Security Management Systems - British Department of Trade and Industry Commercial IT Group 1993
- Managing Security of Information - International Federation of Accountants Information Technology Committee 1998
- Electronic Commerce – Trends, Technology and the Security, Control and Audit Implications - Institute of Internal Auditors 1998
- Practice for Securing Critical Information Assets - 2000
- Guide for Developing Security Plans for Information Technology Systems - NIST Computer Security Online Special Publication
- Canadian Handbook on Information Technology Security (MG-9) - Communications Security Establishment
- Managing the Security of Information An Executive Guide - International Federation of Accountants (IFAC)
- Information Security Management – Practices of Leading Organizations - US General Accounting Office – Executive Guide
- Information Security Risk Assessment Guide – Practices of Leading Organizations - US General Accounting Office – Exposure Draft
- Information Technology Security Maturity framework - US CIO Council Security Subcommittee
- Technical Security Standards for Information Technology - RCMP 1997.

(SOURCE: Hunter *Information Security: Raising Awareness* (2000) 36).

A BRIEF OVERVIEW OF THE SCOPE AND APPLICATION OF THE THREE MOST IMPORTANT INFORMATION SECURITY STANDARDS:

International Organisation for Standardisation
ISO 17799

ISO 17799 is a comprehensive set of controls comprising of best practices in information security. It is intended to serve as a single reference point for identifying the range of controls needed for most situations where information systems are used in industry and commerce. It is suitable for use in any size organisation. It treats information as an asset that, like other important business assets, has value to the organisation and consequently needs to be suitably protected.

Information security is characterised within ISO 17799 as the preservation off:

- Confidentiality – Ensuring that information is accessible only to those authorised to have access to it;
- Integrity – Safeguarding the accuracy and completeness of information and processing methods; and
- Availability – Ensuring that authorised users have access to information and associated assets when required.

Information security protects information from a wide range of threats in order to ensure business continuity, minimise business damage, maxamise return on investment and capatalise on business opportunities.

Security is achieved by implementing a suitable set of controls, which consists of policies, procedures, organisational structures and/or software functions.

ISO 17799 comprises of ten principal sections:

(1) Business Continuity Management (BCM);
(2) System access control;
(3) System development and maintenance;
(4) Physical and environmental security;
(5) Compliance;
(6) Personnel security;
(7) Security organisation;
(8) Computer and operations management;
(9) Asset classification and control; and
(10) Security policy.

Information Systems Audit and Control Foundation / IT Governance Institute
Control Objectives for Information and Related Technology (COBIT)

COBIT starts from the premises that IT needs to deliver the information that the enterprise needs to achieve its objectives. In addition to promoting process focus and process ownership, COBIT looks at fiduciary, quality and security needs of enterprises and provides for seven information criteria that can be used to generically define what the business requires from IT:

(1) Effectiveness;
(2) Efficiency;
(3) Availability;
(4) Integrity;
(5) Confidentiality;
(6) Reliability; and
(7) Compliance.

COBIT further divides IT into 34 processes belonging to four domains, namely:

(1) Planning and Organising;
(2) Acquiring and Implementing;
(3) Delivery and Support; and
(4) Monitoring.

For each process, a high-level control objective is defined:

- Identify which information criteria are most important in that IT process;
- Listing which resources will usually be leveraged; and
- Providing consideration on what is important for controlling that IT process.

Organisation for Economic Co-operation and Development (OECD)
Guidelines for the Security of Information Systems and Networks

These guidelines constitute a foundation for work towards a culture of security throughout society. It proposes that all participants adopt a culture of security as a way of thinking about, assessing, and acting on, the operations of information systems and networks.

These guidelines aim to:

- Promote a culture of security;
- Raise awareness about risk to information systems and networks; the policies, practices, measures and procedures available to address those risk; and the need for their adoption and implementation;
- Foster greater confidence amongst all participants in information systems and networks and the way in which they are provided and use;
- Create a general frame of reference that will help participants understand security issues;
- Promote co-operation and information sharing; and
- Promote the consideration of security as an important objective among all participants involved in the development or implementation of standards.

The framework advances nine principles that will aid participant in fostering a culture of security. These principles are: (1) awareness; (2) responsibility; (3) response; (4) ethics; (5) democracy; (6) risk assessment; (7) security design and implementation; (8) security management; and (9) reassessment.

(SOURCE: IT Governance Institute "Information security governance" (last visited 24 July 2003) http://www.ITgovernance.org 24-27).

5. INTERNATIONAL REGULATORY REPORTS AND EMERGING STANDARDS ON GOVERNANCE

- Report of the Committee on the Financial Aspects of Corporate Governance (Cadbury Report 1992)
- Internal Control: Guidance for Directors on the Combined Code (Turnbull Report 1999)
- Organisation for Economic Co-operation and Development: OECD Principles of Corporate Governance
- King II Report on Corporate Governance 2002
- JSE New Listing Requirements 2003

(SOURCE: IT Governance Institute "Board briefing on IT governance" (last visited 24 July 2003) http://www.ITgovernance.org 40-41).

ANNEXURE B: SCORECARD CHECKUP

To evaluate your organisation's approach to scorecards and the scorecard itself, the following questions should be addresses:

1. Is there a strategic vision?
2. Does the scorecard have executive buy-in?
3. Do your initiatives and measurements tie into your strategy?
   (Measurement motivates. It says that the things that are being measured are important to the company's success. Rewards will motivate employees to improve performance)
4. Does your compensation program link to strategy?
5. Do you have a real purpose for implementing the scorecard?
6. Are you communicating the scorecard's importance to every level of the organisation? and
7. Are you revisiting measurements to confirm their continued relevance?
   (De-emphasise certain measures, re-emphasise others, as the market situation changes).

(Source: Young "Score it a hit" (Nov 15 1998) *CIO Enterprise Magazine* 8-9).

ANNEXURE C: BENCHMARKING CHARACTERISTICS AND CONDITIONS FOR SUCCESS:

Benchmarking is a

Continuous
Ongoing
Long-term;

Systematic
Structural
Formal
Analytical
Organised

process for

Evaluating
Understanding
Assessing
Measuring
Comparing

the

Business practices
Products
Services
Work processes
Operations
Functions

of

Organisations
Companies
Institutions

that are

Recognised
Acknowledged
Identified

as

Best-in-class
World-class
Representing best practices

for the purpose of

Organisational comparison
Organisational improvement
Meeting or surpassing industry best practices
Developing products/process objectives
Establishing priorities, targets and goals

(SOURCE: Van der Zee *Measuring the Value of Information Technology* (2002) 144).

ANNEXURE D: INFORMATION SECURITY STRATEGY SCORECARD

1. Scope	1 Totally Unclear	2. Rather Vague	3. Basically Understandable	4 Rather Clear	5 Totally Clear

How well does the plan cover all relevant issues, including current and future products and services, the consideration of known and possible competitor plans, governmental and environmental conditions, community relations, associates' capability, and financial capability of the company to support the plan?

2. Market analysis	1 No	2	3 Somewhat	4	5 Yes

Is the plan based on a thorough analysis of the current and near-term market dynamics? Is it focused on increasing current market share or on finding new markets for current capabilities?

3. Imagination	1 No	2	3 Somewhat	4	5 Yes

Does the plan represent out-of-the-box thinking? Is there evidence of new perspectives? Will this plan excite the associates, or will they see it as simply an update of past plans?

4. Alignment	1 Totally Unclear	2 Rather Vague	3 Basically Understandable	4 Rather Clear	5 Totally Clear

Is there a clear line of sight from the corporate imperatives and initiatives through the operating objectives of the business units to the support base of resource management?

5. Flexibility	1	2	3	4	5
	No		Somewhat		Yes

Are there backup plans with alternatives listed in case unforeseeable events occur?

6. Infrastructure	1	2	3	4	5
	No		Somewhat		Yes

Has consideration been given to the technology and process capability of the company to support the plan?

7.Resource	1	2	3	4	5
Allocation	Totally	Rather	Basically	Rather	Totally
	Unclear	Vague	Understandable	Clear	Clear

Is it clear how resources will be allocated in support of each of the major initiatives of the plan?

8. Assumptions	1	2	3	4	5
	No		Somewhat		Yes

Are there unexplained assumptive leaps that leave questions?

9. Responsibility and Accountability	1 Totally Unclear	2 Rather Vague	3 Basically Understandable	4 Rather Clear	5 Totally Clear

Are clear lines of responsibility and accountability laid out in the plan, along with schedules and time lines?

10. E-Business	1 No	2	3 Somewhat	4	5 Yes

Are the forces and potentials of e-world represented, with the listing of e-business and assumptions regarding risks and potential returns on the investment?

(SOURCE: Fitz-endz *The E-Aligned Enterprise* (2001) 134-135).

ANNEXURE E: INFORMATION SECURITY STRATEGY COMMITTEE

It is a well established practice that the board is assisted by committees. The researcher is therefor of the opinion that the board would do well to appoint not only an information technology strategy committee, but also an information security strategy committee, seeing as the success or failure of the discipline information security governance may depend on this.

An Information Security Strategy Committee will:

(i) Consider how the board should become involved in information security governance;
(ii) How to integrate the board's role in information security and business strategy; and
(iii) The extend to which the committee has an ongoing role in information security governance.

The board may however be reluctant to create such a committee because:

(i) Top management is not as well versed in technical issues as it is in other aspects of the business;
(ii) Information security is seen only as an expense and there is insufficient awareness of the actual importance of information security;
(iii) Budget and/or time restrictions exist resulting in a general reluctance to participate in yet another committee;
(iv) CEO's may wish to avoid inviting additional board involvement in enterprise affairs; and

(v) Boards may not wish to undermine the authority of the CEO and CIO.

The Information Security Committee often limits their scope to providing direction to ensure that information security is aligned with current and future business strategies, can also monitor the successful implementation of the strategic plans. This is best achieved by performance measurement – for example through an information security balanced scorecard – enabling management and the board to correct deviations and adjust strategy as needed.

A GENERIC APPROACH ON HOW TO INITIATE AN EFFECTIVE INFORMATION SECURITY STRATEGY COMMITTEE

1. Name

Information Security Strategy Committee of the Board of Directors.

2. Purpose

To assist the board in governing and overseeing the enterpise's information security-related matters.

3. Goal

The committee should ensure that information security is a regular item on the board's agenda and that it is addressed in a structured manner. In addition the committee must ensure that the board has the information it needs to make informed decisions that are essential to achieve the ultimate objectives of information security governance.

These objectives are:

(i) The alignment of information security and the business;

(ii) The delivery of value by information security to the business;

(iii) The measurement of information security performance;

(iv) The management of information security-related risks; and

(v) The sourcing and use of information security resources.

These goals are interdependent and complementary. Achievement of one can be undone by failure of another.

4. Responsibility

The board must receive sound information to make informed decisions. While it is the responsibility of management to provide that information, it is the responsibility of the Information Security Strategy Committee to ensure that management is following through on its obligation. More specifically the committee needs to offer expert insight into and timely advice and direction on topics such as:

(i) The relevance of the latest developments in information security from a business perspective;
(ii) The alignment of information security with the business direction;
(iii) The achievement of strategic information security objectives;
(iv) The availability of suitable information security resources, skills and infrastructure to meet the strategic objectives;
(v) Optimisation of information security costs;
(vi) The role and the value delivery of external information security outsourcing;
(vii) Risk, return and competitive aspects of information security investments;
(viii) Progress on major information security projects;
(ix) The contribution of information security to the business;
(x) Exposure to information security risks, including compliance risks; and
(xi) Containment of risks.

5. Authority

The Information Security Strategy Committee operates at board level but does not assume the board's governance accountability nor does it make final decisions. Neither does it play a role in the day-to-day management. It acts solely as an advisor to the board and management on current and future information security-related issues.

The Information Security Strategy Committee must work in partnership with the other board committees, specifically the IT Strategy Committee, and management to provide input to, review and amend the aligned corporate and information security strategies. Possible partnerships are with:

(i) The Audit Committee;

(ii) The Business Strategy Committee, on value delivery and alignment; and

(iii) The Compensation Committee, on performance measurement.

Executive management drives strategy development and takes responsibility for implementing the strategy after obtaining input and approval from the board and the relevant committees.

6. Membership

The Information Security Strategy Committee is composed of a chairman, several board and non-board members and ex-officio representation of key executives. The chairman should be a board member. The members should be selected on the basis of their knowledge and expertise in understanding the business impact of information and related technology.

To ensure that there is enough technical expertise in the committee, the board may choose to select information security external advisors. Regardless of the number of specialist members, it is important that at least two board members remain active in the committee so the board is adequately represented.

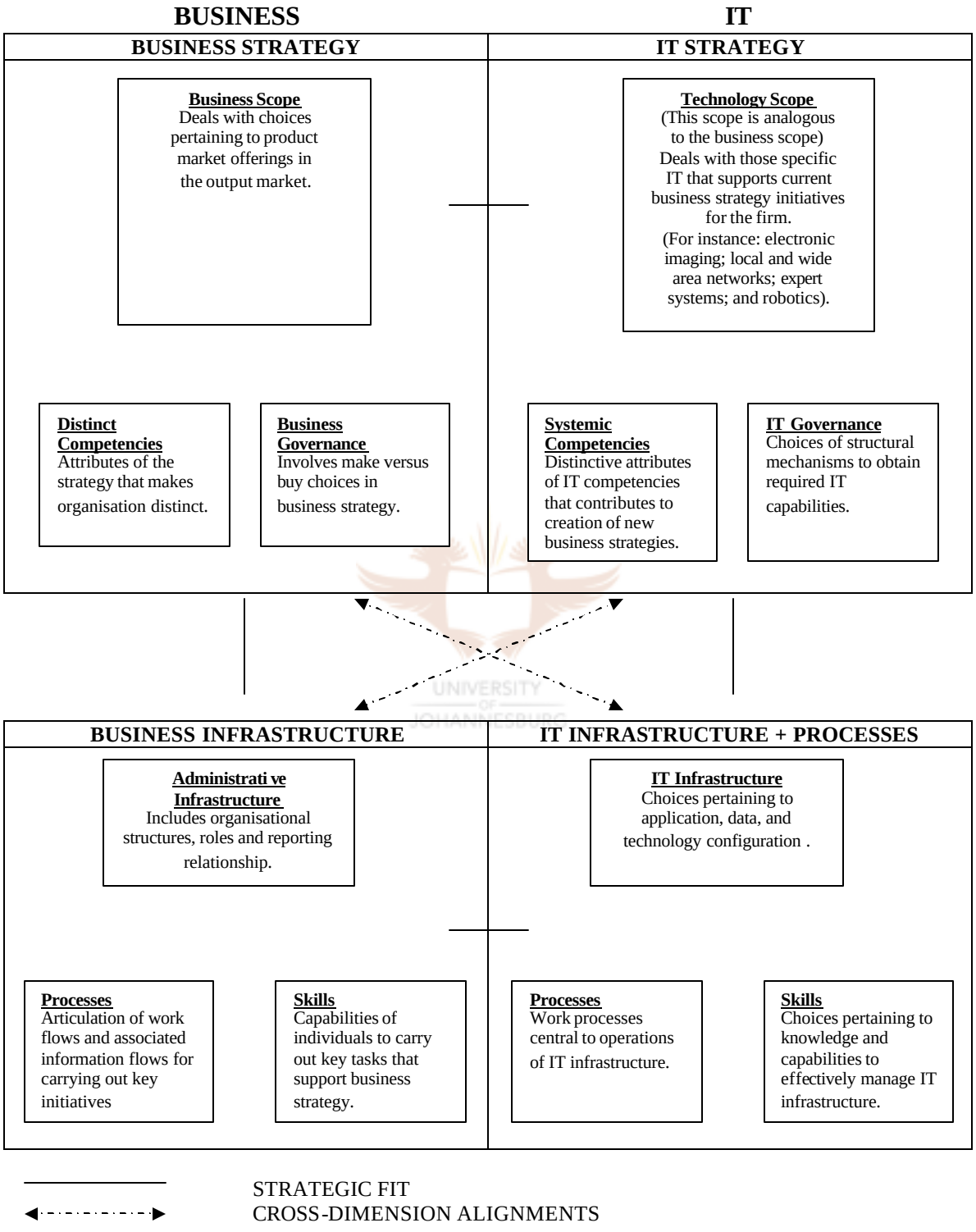
7. Meetings

The Information Security Strategy Committee should meet when needed and as often as needed to accomplish its duties. The committee should report its findings and recommendations to the board. In addition the committee's meeting agenda, minutes and

supporting documents should be provided to the board so that board members not sitting on the committee may submit their comments to the committee chairman.

(SOURCE: IT Governance Institute “IT strategy committee” (last visited 24 July 2002) http://ITgovernance.org 1-2).

ANNEXURE F: HENDERSON AND VENKATRAMAN'S STRATEGIC ALIGNMENT MODEL



(SOURCE: Henderson and Venkatraman "Strategic alignment: leveraging information technology for transforming organisations" (1993) *IBM Systems Journal* Vol 32 no 1 5).

ANNEXURE: G: ALIGNMENT CHECKUP

You know you're in a non-aligned company when…

(i) Meetings and people are political;
(ii) People are not focused on what they can do together;
(iii) People hoard information;
(iv) People go off by themselves to develop ideas and projects;
(v) There is a lot of conversation about how "we need to communicate better; and
(vi) There is a lot of finger-pointing.

You know you are in an aligned company when:

(i) Your success is team success;
(ii) Peer review is of a 360 degree nature;
(iii) The corporate culture values enterpreneurship-spin-offs and risks are encouraged;
(iv) Failure is part of the learning process;
(v) People are applauded for sharing what they have learned from a failed hypothesis; and
(vi) There are no rules or hierarchy about idea generation.

(SOURCE: Glasser "The gulf between" (last visited 24 July 2002) http://www.cio.com 6).

ANNEXURE H: RISK ASSESSMENT QUESTIONNAIRE

Measuring the compliance level with the information security awareness and training program.

INFORMATION PROTECTION PROGRAM AND ADMINISTRATION ASSESSMENT QUESTIONNAIRE

Rating Scale:

1 = Completed
2 = Being implemented
3 = In development
4 = Under discussion
5 = Haven't begun

FACTORS	RATING / VALUE				
	1	**2**	**3**	**4**	**5**
A. ADMINISTRATION					
1. A Corporate Information Officer (CIO) or equivalent level of authority has been named and is responsible for implementing and maintaining an effective IP program.	1	2	3	4	5
2. An individual has been designated as the organisation's information protection coordinator (OIPC) and has been assigned overall responsibility for the IP program.	1	2	3	4	5
3. The OIPC reports directly to the CIO or equivalent.	1	2	3	4	5
4. IP is identified as a separate and distinct budget item	1	2	3	4	5

(minimally one to three percent of the overall ISO budget).

5.	Senior management is aware of the business need for an effective program and is committed to its success.	1	2	3	4	5
6.	Each business unit, department, agency, ect. has designated an individual responsible for implementing the IP program for the organisation.	1	2	3	4	5

B. PROGRAM

1.	The IP program supports the business objectives or mission statement of the enterprise.	1	2	3	4	5
2.	An enterprise-wide IP policy has been implemented.	1	2	3	4	5
3.	The IP program is an integral element of the enterprise's overall management practices.	1	2	3	4	5
4.	A formal risk assessment process has been implemented to assist management in making informed business decisions.	1	2	3	4	5
5.	Purchase and implementation of IP countermeasures are based on cost/benefit analysis utilising risk analysis input.	1	2	3	4	5
6.	The IP program is integrated into a variety of areas both inside and outside the "computer security" field.	1	2	3	4	5
7.	Comprehensive information-protection policies,	1	2	3	4	5

procedures, standards, and guidelines have been created and disseminated to all employees and appropriate third parties.

8. An ongoing IP awareness program has been implemented for all employees. 1 2 3 4 5

9. A positive, proactive relationship between IP and audit has been established and is actively cultivated. 1 2 3 4 5

C. COMPLIANCE

1. Employees are made aware that their data processing activities may be monitored. 1 2 3 4 5

2. An effective program to monitor IP program-related activities has been implemented. 1 2 3 4 5

3. Employee compliance with IP-related activities is a performance appraisal element. 1 2 3 4 5

4. The ITD Project Team members have access to individuals who have leading-edge hardware/software expertise to help the Project Team, as needed. 1 2 3 4 5

5. The application development methodology addresses IP requirements during all phases, including the initiation or analysis (first) phase. 1 2 3 4 5

6. The IP program is reviewed annually and modified where necessary. 1 2 3 4 5

OTHER FACTORS

1.

2.

3.

TOTAL SCORE

Interpreting the total score: Use this table of risk assessment questionnaire score ranges to assess resolution urgency and related actions:

If the score is…	And …	The assessment rate is…	Action might include…
21 to 31	Most activities have been implemented Most employees are aware of the program	Superior	Annual reviews and reports to management Annual recognition days (Computer Security Awareness Day) Team recognition may be appropriate
32 to 41	Many activities have been implemented Many employees are aware of the program and its objectives	Excellent	Formal action plan must be implemented Obtain appropriate sponsorship Obtain senior management commitment
42 to 62	Some activities are under developed An IP team has been identified	Solid	Identify IP goals Identify management sponsor Implement IP policy
63 to 83	There is a plan to begin planning Some benchmarking has begun	Low	Identify roles and responsibilities Conduct formal risk analysis
84 to 105	Policies, standards, procedures are missing or not implemented Management and employees are unaware of the need for a program	Poor	Conduct risk assessment prioritize program elements Obtain budget commitment Identify OIPC

(SOURCE: Tipton and Krause *Information Security Management* Vol 1(2000) 210-211).

ANNEXURE I: SAMPLE INTERVIEW QUESTIONS

(1) Who are valid users?

(2) What is the mission of the user organisation?

(3) What is the purpose of the system in relation to the mission?

(4) How important is the system to the user organisation?

(5) What is the system-availability requirements?

(6) What information (incoming and outgoing) is required by the organisation?

(7) What information is generated by, consumed by, processed on, stored in, and retrieved by the system?

(8) How important is the information to the user organisation's mission?

(9) What are the paths of information flow?

(10) What types of information are processed by and stored on the system?

(11) What is the sensitivity level (classification) of the information?

(12) What information handled by or about the system should not be disclosed and to whom?

(13) Where specifically is the information stored and processed?

(14) What are the types of information storage?

(15) What is the potential impact on the organisation if the information is disclosed to unauthorised personnel?

(16) What are the requirements for information availability and integrity?

(17) What is the effect on the organisation's mission if the system or information is not reliable?

(18) How much system downtime can the organisation tolerate? How does this downtime compare with the repair/recovery time? What other processing communications options can the user access?

(19) Could a system or security malfunction or unavailability result in injury or death?

(SOURCE: National Institute of Standards and Technology, Stoneburner, Goguen, and Feringa *Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology* Special Publication 800-30 (October 2001) A-1).

ANNEXURE J: QUANTITATIVE AND QUALITATIVE RISK ASSESSMENT – A COMPARISON (SOURCE: NIST Stoneburner, Goguen, and Feringa *Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology* Special Publication 800-30 (October 2001) 23).

	Quantitative Risk Assessment	**Qualitative Risk Assessment (QRA)**
CONTENT	The term "quantity" is defined by the Oxford dictionary as the property of things that is estimated by some sort of measure, having a size, extension, weight, amount, or number. Within the IT risk analysis realm the process of Quantitative Risk Assessment attempts to allocate an numeric value to each element/component of the risk assessment process, as well as to the potential loss/damage that might be suffered. Therefor when every element of the risk assessment process have a corresponding numeric value you will encounter a fully quantitative process. For instance a numeric value will be assigned to the cost of controls, value of asset, frequency of threat ect.	The qualitative approach is a much more subjective approach, usually undertaken when reliable data is not available. It will classify risk in general terms such as high, medium or low, and will rely heavily on the experience and expertise of those conducting the assessment. It will highlight those areas that need immediate attention, but it will not quantify the extend of the impact if a threat materialises.
RESULT(S) DELIVERED BY APPROACH	The quantitative approach will result in quantifiable results indicating the extend of the impact. These results may however be complex and require further interpretation by qualified persons.	This approach does not assign any numeric values to the components of the risk assessment process. It rather endeavours to prioritise risk elements in subjective terms.
FACTORS THE APPROACH WILL TAKE INTO CONSIDERATION	The quantitative approach is used to appraise the cost of the risk, as well as the cost of risk mitigation/reduction techniques in pecuniary terms, by taking into account the following factors: (a) Probability that the threat will materialise; (b) Cost of losses suffered or damages incurred; and (c) Cost of implementing controls and/or safeguards to mitigate the risk.	The qualitative risk assessment process will determine what level of protection is required for a specific asset by performing the following tasks, and taking certain factors into account: (a) Assessing the threats and vulnerabilities to organisational assets; (b) Determining the likelihood of a threat materialising; (c) Estimating the cost attached to a threat materialising; and (d) Appraisal of controls and safeguards that may be implemented to reduce the risk of the threat materialising.
ADVANTAGES	The approach is based on accurate, objective mathematical calculation, and delivers results expressed in precise monetary/percentage terms. One of the most important facets of this approach is that the value of the asset is determined in specific monetary terms. A cost-benefit analysis is of crucial importance for the success of this process.	No complicated mathematical calculations or formulas are involved. An accurate calculation of: (1) the monetary value of the information; and (2) the frequency of threat materialisation, is not required. This approach is much more flexible, and allows for the participation of technical, as well as non-technical staff.
DISADVANTAGES	The calculations that need to be performed are very elaborate. The approach itself is not flexible and requires the knowledge and experience of skilled personnel. It also requires a large amount of preparatory work to be performed. Therefor it places a large burden on the resources of the organisation. Past practice have indicated that this approach only functions effectively in conjunction with automated tools.	The results delivered by this approach are very subjective, and will be influenced, and determined by the team assembled to perform the risk assessment. This approach is imprecise. Risk mitigation is very hard to perform due to the absence of a cost-benefit analysis.

ANNEXURE K: SAMPLE RISK ASSESSMENT REPORT OUTLINE

EXECUTIVE SUMMARY

1. Introduction

(i) Purpose

(ii) Scope of this risk assessment

Describe the system components, elements, users, field site location, and any other detail about the system to be considered in the assessment.

2. Risk Assessment Approach

Briefly describe the approach used to conduct the risk assessment, such as –

(i) The participants (eg. risk assessment team);

(ii) The technique used to gather information (eg. tools, questionnaires); and

(iii) The development and description of the risk scale (eg 3x3; 4x4; or 5x5 risk-level matrix).

3. System Characterisation

Characterise the system, including hardware, software, system interfaces, data and users. Provide connectivity diagram or system input and output flowchart to delineate the scope of this risk assessment effort.

4. Threat Statement

Compile and list the potential threat-sources and associated threat actions applicable to the system assessed.

5. Risk Assessment Results

List the observations (vulnerabilities/threat pairs). Each observation must include –

(i) Observation number and brief description;
(ii) A discussion of the threat-source and vulnerability pair;
(iii) Identification of existing mitigating security controls;
(iv) Likelihood discussion and evaluation (eg. high, medium, or low likelihood);
(v) Impact analysis discussion and evaluation (eg. high, medium or low impact);
(vi) Risk rating based on the risk-level matrix (eg. high, medium or low risk level); and
(vii) Recommended controls or alternative options for reducing risk.

6. Summary

Total number of observations. Summarise the observations, the associated risk levels, the recommendations, and any comments in a table format to facilitate the implementation of recommended controls during the risk mitigation process.

(SOURCE: National Institute of Standards and Technology Stoneburner, Goguen, and Feringa *Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology* Special Publication 800-30 (October 2001) B-1-B-2).

ANNEXURE L: INFORMATION SECURITY POLICY

(Sample information security policy of the fictitious company Starcross Inc)

Starcross, Inc.

INFORMATION SECURITY POLICY

Author(s):	Security Team	Policy Effective Date – July 31, 1999
Approval Authority:	Executive Committee for Security	Policy Last Revised – July 31, 1999

INTRODUCTION

The widespread implementation and use of networks and a distributed client/server processing environment are accompanied by new risks and exposures. Networks provide greater flexibility for accessing and sharing information and resources and for performing processing at the desktop. These advantages to networking also increase the exposure of sensitive information and make it necessary to implement control strategies to maintain information confidentiality, integrity, and availability.

This document contains a high-level statement of Starcross, Inc.'s information security intentions, expectations, and objectives, and the necessary implementation strategy for their attainment. This policy is the foundation for all information security activities, including enterprise security architecture development and implementation. It focuses not only on the technology for the storage, processing, and transmission of LAN-based information, but also on administrative and operational practices for the protection of all information, data, files, and processing resources owned by Starcross. All information,

data, applications, networks and equipment (including PCs and printers) are the property of Starcross and is provided to its employees so that they can conduct their job responsibilities effectively. These assets should be treated with privacy and confidentiality when conducting business and should not be made available or accessible to anyone outside the enterprise without specific written permission of the Chief Information Officer.

This policy is the property of Starcross. It was developed under the direction of the Chief Information Officer by the Security Team comprised of network, administrative, and information systems representatives. It is intended for distribution to all employees and users of information systems at Starcross locations.

TABLE OF CONTENTS

1.0 POLICY

1.1 Information Security Policy

Information Assets

Starcross information and information processing infrastructure are vital assets requiring protection commensurate with their value. Organisational information, applications, systems, and networks must be actively managed to ensure security, confidentiality, integrity, and availability.

Accountability

The administrative and departmental computing environments will maintain consistent standards for establishing the accountability and authenticity of system users which will be compatible with internal accounting control standards prescribed by Starcross, Inc.

These environments will develop unique standards for protecting information, applications, systems, and network resources contained within these environments that will be commensurate with fulfilling the mission of Starcross and maintaining the integrity of those critical resources.

To maintain accountability for system access, we will implement the following:

- All individuals with access to the systems will use a user ID that has been specifically assigned to that individual. Sharing of user IDs is prohibited except in specific, approved situations. Written justification for such an

ID is required and approval for use will be granted only by senior management.

- All individuals with network, system, and application user IDs will retain a confidential password that will be used to authenticate the identity of the individual. Intentional disclosure or sharing of passwords is prohibited. To meet the needs of some applications, certain terminals can utilise a location or station password, with strictly limited access to applications. User IDs will be required on all documents generated or modified.

Information Access

All access to information is to be authorised by responsible management, with access granted or revoked based on business requirements only. Access to administrative data will be granted to Starcross employees only. Individuals outside of Starcross can be authorized access to Starcross data only if that authorization is granted by the appropriate Department Manager and the Chief Information Officer.

Access and update capabilities and restrictions will apply to all Starcross administrative, departmental, and operational data, stored on the administrative, departmental, and operational systems computing facilities. Security measures apply to all systems developed or maintained by Starcross locations, departments, organisations, affiliates, outside vendors, or contractors.

The appropriate Department Manager and the System Administrator are responsible for authorising access to systems and information, verifying information integrity, and controlling extracted information. Management is responsible for developing secure processing systems and operating these systems in a controlled environment. Employees are required to comply with management's direction for the use and protection of information technology processing systems and information. Employees must be kept aware of the importance of information security. All managers and employees are required to act with urgency and diligence to fulfill these requirements.

Risks must be evaluated to determine the optimum level of control required for each type of information technology system. Adequate controls are to be included to ensure that information security, confidentiality, integrity, and availability are achieved.

Violation of Policy

Violation of this policy should be brought to the immediate attention of the Security Officer. Violations should be reported to Bill Gernsey. Instances of known or suspected employee infidelities should be reported to the Security Officer and the Chief Information Officer. The Security Officer will work with Department Managers, LAN Administrators, and the Security Team to ensure that the problem is resolved an to address necessary steps to eliminate future violations. An escalation process will define the course of action for all violations consistent with the severity of the violation.

Detailed security standards and procedures are documented in the Starcross Security Standards and Procedures Manual (SS&PM).

STARCROSS RESERVES THE RIGHT TO DISCIPLINE, TERMINATE, SUSPEND, OR PROSECUTE, AT ITS DISCRETION, INDIVIDUALS WHO VIOLATE THE INFORMATION SECURITY POLICY.

1.2 Policy Objectives

1.2.1 Security Management

The Security of corporate information, applications, systems, and networks is fundamental to the continued success of Starcross. Security management seeks to establish controls and measures to minimize the risk of loss of information and system resources, corruption of data, disruption of access to the data, and unauthorised disclosure

of information. Security management is achieved through effective policies, standards, and procedures that will ensure the confidentiality, integrity, and availability of Starcross information, applications, systems and networks for authorized users.

1.2.2 Confidentiality

Confidentiality relates to the protection of information from unauthorized access regardless of where it resides or how it is stored. Information that is sensitive or proprietary needs to be protected at a higher level than other information. Policies are in place to identify what information is confidential and the period of time it should remain confidential. The SS&PM provides a framework for classifying the confidentiality of data according to its characteristics and indicates associated security requirements for each confidentiality ranking.

1.2.3 Integrity

Integrity is the protection of information, applications, systems, and networks from intentional, unauthorised, or accidental changes. It is also important to protect the processes or programs used to manipulate data. Information should be presented to information owners and users in an accurate, complete, and timely manner. Key to achieving integrity is identification and authentication of all users accessing information, applications, systems, and networks through the use or manual and automated checks. Employees must not take any action which could compromise the integrity of the information, application, system, or network.

1.2.4 Availability

Availability is the assurance that Starcross information and resources are accessible by authorized users as needed. There are two issues relative to availability: denial of services caused by a lack of security controls (e.g., destruction of data or equipment, computer virus), and loss of services from information resources due to natural disasters

(e.g., storms, floods, fires). Denial of services is addressed as a part of security management and will be discussed later in this document. Loss of services is addressed as part of the Business Continuation Planning process. The SS&PM provides a framework for classifying the availability of data according to its characteristics and indicates associated security requirements for each availability ranking.

1.3 Policy Scope and Responsibilities

1.3.1 Policy Scope

This policy applies to all employees, vendors, contractors, and consultants who create, distribute, access, or manage information by means of Starcross' information technology systems, including personal, department, or corporate computers, networks, and communication services by which they are connected. It equally applies to individuals and enterprises, who by nature of their relationship to Starcross, are entrusted with confidential or sensitive information. This policy addresses all aspects of information security and continuity from initial design of a system through implementation and operation. It also addresses any device used to store, process, or communicate Starcross proprietary or other protected information.

It is the intent of Starcross management to provide direction and an environment that facilitates the communication and use of information within the bounds of sound business practices, and the legal or regulatory restrictions that apply. Security policies, standards, procedures, and business continuation plans have been developed to provide consistency in implementing controls. These define protection requirements or provide guidance to management responsible for implementing controls within their business functions. It is the intent of this Policy to facilitate the exchange of information and computing resources while balancing the need for protecting information with the cost of implementation.

1.3.2 Security Officer

The Security Officer of Starcross has overall responsibility for information security matters. These responsibilities are to:

- Ensure appropriate user access and authentication controls are in place;
- Ensure that the documented security policies, standards, and procedures are reviewed, updated and maintained periodically by appropriate individuals;
- Evaluate security exposures, misuse, or non-compliance situations and ensure implementation of security controls to address those incidences;
- Ensure that all department Security Coordinators understand and execute their security responsibilities in accordance with related policies, standards, and procedures;
- Organise and conduct periodic Security Team meetings; and
- Develop and implement the Security Awareness Program with assistance from the Security Team members.

1.3.3 Security Coordinators

Security Coordinators will be assigned within each site or department. The Coordinator's primary responsibility is to ensure that appropriate user access within the scope of their business function is maintained. Additional responsibilities include:

- Ensure that Application Access Forms are initiated for existing and new users within the respective departmental area;
- Ensure that access is modified or deleted when employees and non-employees operating within their business function or site are transferred or terminated;
- Conduct user security awareness within their departmental function;

- Ensure that the Starcross Confidentiality Agreement and Exit Interview Form are signed by all users operating within their department or area of responsibility;
- Actively participate as a member of the Security Team; and
- Coordinate with the Security Officer on all security-related matters.

1.3.4 Security Team

The Security Team is comprised of the Security Officer, Security Coordinators, Network, Applications, and Internal Audit representatives within Starcross. This team is responsible for communicating to management the risk control strategies that are being considered for implementation across sites and to report management's concerns about these protection measures. Specific functions of the team, together with operating management, are to:

- Represent particular security and business continuation issues and concerns within each Starcross site;
- Identify risks within their area of concentration and ensure that appropriate controls are implemented to address these risks;
- Recommend, review, and approve all security policies, standards, and procedures that will be implemented across sites; and
- Develop and implement an Information Security Awareness Program for all information technology administrators, development personnel, users, and their management, and administer the implementation of this program within their area.

1.3.5 Executive Committee for Security

The Executive Committee for Security is comprised of director-level management responsible for reviewing all security plans relating to the protection of Starcross systems and electronic information assets. In this role, the Executive Committee for Security is

responsible for reviewing the Policy and for ensuring that all implementation plans, procedures, and standards are consistent with the overall risk management and protection expectations of Starcross' senior management. When appropriate, the Executive Committee for Security will forward recommendations for approval to the Board of Directors.

1.3.6 Help Desk

The Help Desk will maintain the Security Policy and the Security Standards and Procedures Manual (SS&PM) online. The Help Desk will be responsible for answering security related questions in accordance with policy, standards, and procedures and for directing security-related issues to the appropriate department management in accordance with Security Incident Escalation Procedures as defined in the SS&PM. The Help Desk will also provide password management assistance to include security awareness to users in strengthening and protecting passwords.

1.3.7 Departmental Management

Department Management in this document refers to Starcross managers who are responsible for functional business areas. Reference to Departmental Management generally means the head or a designated person who has the responsibility and authority to act on behalf of senior management. This person is also considered the owner of the information. Departmental Management is responsible for establishing the overall security strategy for department information. This includes determining the security classification of information owned by the department. Classifications will indicate the level of sensitivity and availability required for the information. In addition, Department Management is responsible for authorising the level of access to information within each respective department function.

1.3.8 Application Coordinators

Application Coordinators are jointly established by department and systems management and report directly to these managers. These Coordinators are responsible for assisting the Department Manager in implementing and managing information technology security policies, procedures, standards, and departmental guidelines within their functional area. The Coordinator serves as the principal liaison between their department and the Network Administrators.

1.3.9 Human Resources Department

Human Resources is responsible for managing and coordinating hiring, termination, and disciplinary practices within Starcross. Human Resources and Departmental Management are responsible for providing timely information to the enterprise LAN manager about employee termination or transfers so that appropriate steps can be taken to revoke or change access to systems and information. Human Resources will also ensure that new hires will be given the opportunity to read both the Security Policy and the Information Security Policy Acknowledgment Form and sign the Information Security Policy Acknowledgment Form. In addition, Human Resources will ensure that the Exit Interview and Reaffirmation of Confidentiality Obligations is read and signed by all employees leaving the company.

1.3.10 Internal Audit

The Internal Audit function is performed by the Internal Audit Department who is responsible for periodically reporting on the effectiveness of information technology security policies, standards, and procedures and evaluating the appropriateness of risk management techniques utilised by Starcross. Annually, in cooperation with Starcross management, Internal Audit identifies departments, business functions, systems, or applications to be reviewed, and conducts inquiries and tests to determine the level of

risk, as well as the effectiveness of controls and compliance with policies, standards, and procedures established by Starcross management. Internal Audit is also responsible for ensuring compliance with software licensing agreements. Internal Audit reports to management their results and, where applicable, recommendations for improving risk management capabilities as well as any instances where policies, procedures, and standards are not effectively implemented. Internal Audit provides written reports to Halford and Associates, Starcross' external auditors, and the Chief Financial Officer.

1.3.11 Information Users

Information users include all employees of Starcross who access or receive information produced, stored, or communicated by Starcross' information technology systems. Information users also include all individuals, who by nature of their relationship with Starcross (e.g., contractors, vendors, service providers, consultants, etc.) are entrusted with sensitive or confidential information. Information users are responsible for compliance with the Information Security Policy and individual standards and procedures contained within the Security Standards and Procedures Manual.

Noncompliance to the Security Policies and Standards will be investigated and disciplinary actions will be administered by the appropriate immediate manager where the infraction has occurred. Human Resources will be involved as required. Disciplinary actions can range from a verbal warning to employment termination, suspension, or prosecution.

Information users who are not Starcross employees are also bound by the signed agreement between Starcross and the individual or company that addresses non-disclosure of Starcross information.

1.4 Implementation

1.4.1 Information Resources

Information resources including computer software and support systems should be protected appropriately to maintain the sensitivity and critical nature of information that is processed, stored, or communicated. Information systems should be protected in such a manner to ensure that unauthorised persons are not able to directly access the device and either cause physical damage or modify internal components that could affect the results of computing or other processes. Environmental and security controls should be appropriate for the level of risk. An assessment that balances risk with the cost of implementing the control should be completed when determining what security and environmental controls are appropriate.

Information resources should be classified by the designated data owner using the risk assessment guidelines described in the SS&PM. Information assets are classified in order to provide a means of communicating the level of protection to be provided. Information security requirements will vary with the sensitivity and level of importance of the information or the systems associated with that information.

Users are responsible for adhering to copyright, patent laws, and license agreements for intellectual property. Violations of authorial integrity, which may be grounds for sanction, include: plagiarism, invasion of privacy, unauthorised access, trade secrets, and copyright violations.

Communication facilities and equipment should be protected from unauthorised modification and tampering to ensure that messages in transit are not modified or received by unintended parties or that communication services are not interrupted. Communication facilities can include all equipment rooms and wiring closets and may include facilities and resources provided by third-party service providers.

Questions concerning the appropriateness of physical and environmental controls should be addressed to the Security Officer.

1.4.2 System and Information Ownership

Starcross is the owner of all information, applications, systems, and software that is developed, used, or distributed to employees or designated representatives of entities operating as business partners. Although Starcross maintains the ultimate ownership responsibility, certain managers are responsible for executing this responsibility.

Systems and information owners are responsible for identifying and managing risks relating to the security, integrity, and continuity of information, and for the business processes and system functions that create, modify, delete, or use this information. They are responsible for assessing the level of risk to Starcross for providing access to information, as well as for determining the impact to the organisation if information, business processes, or system functions were not available or if they are misused.

The level of security, integrity, and continuity risk needs to be communicated by the owner to individuals or groups responsible for implementing Starcross security and continuity controls. Business process integrity controls as well as departmental security and continuity measures may need to be implemented by owners to support Starcross protection plans and procedures. Local sites will be responsible for security on their portion of applications, systems, and networks.

Periodically, the Data Owner and the Security Officer will review the current set of access and update capabilities granted to each individual on the system in order to ensure that the appropriate level of access has been granted and that no changes are necessary. Data Owners are indicated in Appendix A of the Security Standards and Procedures Manual.

1.4.3 Access to Systems and Information

All access to information and systems is provided based on business need. Information owners, as part of their management responsibility, are required to review all requests for access to information or systems, and to verify that such access meets a legitimate business need. Approval for access needs must be communicated to the Network Administrator or the department's Security Coordinator as required for implementation. An Application Access Request Form will be filled out by the user's Departmental Manager. This form will indicate the files and applications that the user should be permitted to access. The Application Access Request Form will be signed by (1) the Departmental Manager and (2) the Application/Resource Coordinator. The Information Security Policy Acknowledgment Form will be used to acknowledge that each user has read the Information Security Policy and understands the responsibilities in connection with the Policy and the consequences of a policy infraction. Examples of the above described forms are located in the SS&PM. These completed forms will be retained by the Security Officer.

Access requests for information between departments must meet the same test of business need. When making the decision to either grant or deny access, the owner should consider the benefits to Starcross for granting access, the type of access that is required, and the business risk associated with such access.

Access to certain sensitive information needs to be restricted. Owners may require that information provided to another department is not distributed to other groups without prior approval. Owners may also designate a retention period during which the information or access may be authorised and after which all access is to be revoked. Owners must approve or deny all access requests.

When approval for outside access to Starcross information is granted, detailed instructions must be provided to the recipient, notifying them of any security requirements including the need to maintain the confidentiality of the information, requirements for distribution of the information within their organisation, and procedures

for destruction or return of the information following the period of access. All non-employees will sign a non-disclosure agreement. More details can be found in SS&PM.

Human Resources will immediately notify the Managers of Information Services of all employee terminations via e-mail. A monthly report detailing employee terminations and resignations will be sent from Human Resources to the Manager of Information Services to confirm the deletion of user IDs. This list will indicate the employees whose LAN and application user IDs should have been removed from the system upon initial notification. The Manager of Information Services will notify the LAN and Application Coordinators, who will, upon notification, disable the user IDs immediately. A Coordinator will be assigned to ensure that all contractor, vendor, and consultant user IDs are properly disabled upon leaving the company. When a Department Manager is notified of an employee termination/resignation, they should review the disposition of the user's data and files residing on the network or application directories with the user prior to separation from Starcross. The Manager will notify the LAN and Application Coordinator in writing of those files to be transferred or destroyed. Disposition of any files will follow the guidelines defined by the Documentation Retention Program.

1.4.4 Security Monitoring and Enforcement

It is the responsibility of both Network and Application Coordinators to implement appropriate measures to detect attempts to compromise the security or integrity of information or information technology systems. When implementing monitoring capabilities, consideration should be given as to what situations are to be monitored based on the extent of risk, the most effective means for monitoring security activities, the resources available for monitoring, and system constraints that limit the ability to monitor security events. If appropriate measures are not available within a system environment to effectively monitor security events, additional software should be installed or additional controls to mitigate security risks should be implemented.

When activity occurs that is in conflict with security policies and standards, Application Coordinators or Network Administrators should take the appropriate steps to enforce desired security practices. The steps involved range from training of the users, revoking access, altering security parameters, and possibly disciplinary actions.

Due to the likelihood of damage and destruction of information resulting from malicious code including viruses, detection capabilities must include virus detection software within the local area network environment, as well as on systems that are at high risk for infection.

The facts surrounding an intrusion, infection, or system compromise must be documented, reported to the Security Officer, and include the circumstances that led to the discovery of the incident, actions which were immediately taken, the names of persons involved in investigating the incident, and detailed observations about what transpired, what damage was caused, and what systems or files were compromised.

Starcross will enforce and support the Information Security Policy at its discretion by responding to business ethics violations and employee/non-employee infidelities – known or suspected – through disciplinary action, termination, suspension, or prosecution.

1.4.5 Security Awareness Program

It is the responsibility of management to ensure that all users of information understand how to protect company assets, including information and information resources and comply with security policies, standards, and procedures. Supervisors and managers must ensure that persons working within their department understand general information security requirements and that they are sufficiently knowledgeable about the information technology security policies, standards, and procedures to recognize the need for protecting information and the requirements for which they are specifically responsible.

The security Officer with assistance from the Security Team is responsible for developing and implementing an information security awareness program that supports employees awareness.

Managers and supervisors need to be aware of user performance in this area, encourage good security practices, and address inappropriate behaviour. Application Coordinators can assist in implementing specific awareness programs.

1.5 Controls

1.5.1 Risk Assessment

Risk assessment involves identifying the sensitivity and criticality of information and the consequences to Starcross if information is disclosed, modified, or destroyed. Risk assessment techniques can include formal methods of determining the financial and operational impact of a security incident as well as less formal assessment techniques. A risk assessment process should include the following elements:

- A determination of the information assets that need to be protected;
- Evaluation of the sensitivity of the information and the consequences if information is disclosed;
- Evaluation of the criticality of information and the consequences to business processes if information and information processing systems are not available;
- A determination by management of the extent of risk that will be accepted, mitigated, or transferred;
- Development of a risk control strategy; and
- Determination of compliance with regulatory information classifications.

It is the responsibility of management to understand the level of risk to Starcross relating to the confidentiality, integrity, and availability of information and to the controls necessary to effectively mitigate this risk. Risk control measures should address not only the information but the processes that are used to create, modify, report, or distribute information, and the environments under which these processes exist. This process should also incorporate the classification of data/information in accordance with the Starcross SS&PM into one of the following categories:

- Confidential;
- Starcross Business Use Only;
- Public;
- Indefinite;
- Medium-term;
- Long-term; and
- Critical.

The SS&PM provides a framework for classifying the confidentiality, integrity, and availability rankings for data and the necessary security requirements for each classification.

1.5.2 Corporate Policies

These policies will not conflict with any policies established by Starcross. Although there may be some areas where practices differ, the Corporate policy will prevail. Exceptions will be on a case-by-case basis and must be approved by the Executive Committee for Security.

1.5.3 Departmental Procedures and Guidelines

Each department should develop and maintain additional departmental procedures and guidelines that support the overall intent of the Information Security Policy, if necessary to meet special situations. The procedures and guidelines should be specific to the business unit's applications and the security required. Departmental Management is responsible for ensuring that appropriate personnel within the department are familiar with the procedures and guidelines. It should be understood by departmental personnel and particularly the Application Coordinator that their jobs are to be performed in a way that complies with the standards, procedures, and guidelines.

1.5.4 Starcross Policies and Procedures Manual

The Starcross Policies and Procedures Manual provides the general framework for tasks performed in the Information Systems department. This document defines the methodology for any system and application development.

1.5.5 Starcross Security Standards and Procedures Manual

The Starcross Security Standards and Procedures Manual (SS&PM) documents detailed methods for achieving the security objectives stated in this Policy. This manual along with the Information Security Policy helps to define the framework for Starcross' Information Security strategy, architecture, and implementation. It focuses not only on the technology for the storage, processing, and transmission of LAN-based information, but also on administrative and operational practices for its protection in all of its forms both inside and outside of Starcross. This document should be referenced to gain a general understanding of Starcross' approach to security.

(SOURCE: Tudor *Information Security Architecture* (2001) 243-256).

ANNEXURE M: INFORMATION SECURITY POLICY ACKNOWLEDGEMENT FORM

==========

Starcross, Inc.

INFORMATION SECURITY

POLICY ACKNOWLEDGEMENT FORM

Author(s)	Security Team	Policy Effective Date – July 31, 1999
Approval Authority:	Executive Committee	Policy Last Revisited – July 31, 1999
	For Security	Policy Review Date – January 31,2000

INTRODUCTION RESOURCES SECURITY

Information security is the protection of company data, applications, systems, and network resources from accidental or deliberate misuse through unauthorised disclosure, alteration, or destruction.

Information resources include:

1. Printed or written communications and documentation, such as reports, letters, and memos;
2. Online screen transactions;
3. Software applications;

4. Data set files and databases residing on any media, such as tape, disk, diskettes, microfilm, and microfiche;
5. Processing systems to include servers, PC's workstations, and printers; and
6. Network resources.

It is every user's responsibility to guard against unauthorised use, destruction or disclosure of these assets. Every user is responsible for reasonable protection of company information and information resources.

Starcross stores, processes, and disseminates large amounts of critical information. Loss damage, or disclosure of information, applications, systems, or network resources could result in a significant operational or financial loss to the enterprise. It is imperative to ensure the integrity, accuracy, availability, and confidentiality of these resources through the use of effective security controls.

USER RESPONSIBILITIES

Each user of Starcross Inc is responsible for safeguarding the confidentiality and integrity of resources to which he or she has access. The acknowledgement form and the Starcross Information Security Policy applies to all users of the Starcross computer systems, including employees, clients, contractors, and other individuals who have been granted access and authority to Starcross computer systems.

If you have a user-id, you are responsible for the confidentiality of the password, and for any action performed with your user-id.
The following guidelines will be adhered to:

1. Your user-id and password are yours; do not loan them out or share them with others. You are personally accountable for all actions that occur under your user-id.

2. Select an alphabetical password that has both letters and numbers and would not be easily "guessed". Passphrases are the most acceptable, in which a phrase is used in combination with numbers. Do not use repeating characters. Do not use obvious passwords such as your name, your spouse's, children's, or pet's names, days of the week, names of the months, your user-id, birthday, phone, or social security number. Make sure your password is a minimum of eight characters in length and that it is changed a minimum of every 60 days.
3. Memorise your password instead of writing it down and do not store it in programmable function keys.
4. Log out or lock your terminal when leaving it, even for a short period of time. Be sure and log out when you leave for lunch.
5. Keep documents, diskettes, and copies of files containing sensitive data in a secure cabinet, desk, or room, and disposal of them properly when no longer needed. Reformat reusable diskettes containing sensitive data before releasing them for reuse.
6. Ensure that your data and transactions are protected against unauthorised use.
7. If you think your use-id and password have been compromised in any way, immediately change your password, and notify your supervisor or the Security Coordinator for your business area.
8. Report all suspicious activity, breaches in security, and practices not conducive to good data security to your supervisor or Security Coordinator for your business function.
9. Protect the confidentiality of sensitive data when viewing it online.
10. Company computer resources are to be used for company business only. Use for anything other than that for which you are authorised is considered misuse.
11. Computer users should take precautions to prevent the introduction of software viruses into their PC's. Games, files downloaded from bulletin boards and the Internet, and software brought from home are not authorised and increase the risk of loss due to viruses on the network.

SECURITY POLICY ACKNOWLEDGEMENT

Signing this form constitutes acknowledgement by you of your responsibility to guard against unauthorised use or disclosure of company resources or information, and agreement that you will comply with all of the security policies and rules listed in this acknowledgement form and with the Information Security Policy.

Starcross reserves the right to monitor e-mail, voice mail, and processing system activity, transactions, and files to prevent abuse, misuse, or for any other legitimate business reason.

I have read and understand the Starcross Information Security Policy and Acknowledgement Form as presented above.

_____ _____

Signature Date

_____ _____

(Printed Name) Social Security Number

(SOURCE: Tudor *Information Security Architecture* (2001) 257-259).

ANNEXURE N: INFORMATION SECURITY CHECKLIST

1. Has the company designated key personnel for auditing its security policy?
   Have system administrators, network administrators, and security personnel been trained to recognize signs of intrusion?
   (Assign roles and responsibilities)

2. Has the company completed an audit of its information assets to determine what it needs to protect?
   Have tools been implemented for auditing information security?
   (Risk assessment)

3. Has the appropriate level of network security been established, calibrated to the importance of the material to be protected?
   Are secret documents available only on a "need to know" basis? Has a scale been established indicating levels of confidentiality?
   (Risk assessment – information classification)

4. Have access controls for levels of security been implemented and are they being enforced?
   (Risk mitigation)

5. What procedures have been instituted to train employees in the organisation's policy for e-mail and Internet usage?
   Does user education include how to respond to security breaches or other suspicious incidents?
   (Information security awareness and training)

6. Does the company's website follow acceptable standards for information security to ensure transactional integrity?
   Is the web site certified as meeting high-level accepted industry standards?
   (Information security standards - ISO 17799)

7. Are procedures in place to protect the company's computer system from malicious code, such as Trojan horses, network worms, or other computer viruses?
   Do employees know what to do if they receive a virus?
   (Risk management)

8. Is there a standard computer incident reporting form?
   (Risk management)

9. Have tests been run on the website to check for security holes?
   (Risk management - penetration testing)

10. Have servers been reconfigured to block third-party e-mail relays by programmers?
    (Risk mitigation)

11. Does the company have established procedures for informing employees of the organisation's information security policy and of any changes to it?
    (Awareness and training program)

12. Does the company have a disaster recovery procedure in the event of an information intrusion?
    (Risk management – risk mitigation)

(SOURCE: Rustad and Daftary *E-Business Legal Handbook* (2002) 970-971).

ANNEXURE O: ASSESSMENT OF INFORMATION SECURITY GOVERNANCE AT BOARDROOM LEVEL

ASSESSMENT OF THE BOARD'S INVOLVEMENT IN, COMMITMENT TO, AND ACKNOWLEDGEMENT OF INFORMATION SECURITY GOVERNANCE

In order to determine if the board of directors is giving information security governance the attention it deserves the board should answer the following questions:

1. Does your board realize that information security is a board level issue and cannot be left to IT alone? Is your information security strategy aligned with your business strategy?
2. Is there clear accountability for information security in your organisation?
3. Can your board members articulate a clear set of threats and critical assets? How often do you review and update this?
4. Do you know how much is spent on information security and what is it being spent on? Can you measure your return on investment?
5. What would be the impact on an organisation if a serious security incident occurred (Reputation, Revenue, Legal, Operational Performance, Investor Confidence)?
6. How does your organisation see information security as an enabler?
7. Has your business assessed the risk of getting a reputation for slacking in security?
8. What steps have you taken to satisfy yourself that well intended (or not) third parties will not compromise the security of your organisation?
9. How do you obtain independent assurance that information security is managed effectively in your organisation?
10. How do you measure the effectiveness of your information security activities?

(SOURCE: Ernst & Young "Global information security survey" (last visited 24 July 2002) http://www.ey.com/global 8).

ANNEXURE P: INFORMATION SECURITY TOOLBOX

The board of directors need effective tools to implement information security governance within their organisation.

The information security toolbox should include the following items

1. Benchmarks
2. Standards and metrics
3. Integrated risk management technologies and processes
4. Trained and experienced people
5. Links to industry alerts and warnings
6. Processes to assess and react to change and challenge

(SOURCE: IAAC "Information assurance guidelines for boards and senior managers" (last visited 24 July 2002) http://wwwiaac.org.uk 3).

ANNEXURE Q: RESPONSIBILITIES OF THE BOARD AND TOP MANAGEMENT FOR INFORMATION SECURITY GOVERNANCE

Keys:

B = Board of Directors

M = Top Management

Responsibilities of the Board and Top Management for Information Security Governance		
Become informed of the role and impact of information security on the organisation	B/M	Plan
Set direction and expected returns	B	Direct
Determine required capabilities and investments	M	Plan
Assign responsibilities	B/M	Direct
Sustain current operations	M	Organize
Make transformation happen	B/M	Direct
Define constraints within which to operate	B	Direct
Acquire and mobilize resources	M	Organise
Measure performance	B	Control
Manage risk	B/M	Control
Obtain assurance	B	Control

(SOURCE: Appleby "Closing the governance gap bringing boards into the IT equation" (August 2001) Vol 7 Number 7 3).

Questions the board and management should ask themselves in order to assess their own compliance with information security responsibilities:

Directors and top management must educate themselves on information security	- Does information security have visible and measurable board support? - Is the organisation clear where it sees itself in its approach to security and risk? - Is information security importance reflected in investments and programmes?
Ensuring accountability for information security	- Have roles and responsibilities been assigned for information security? - Do you have performance metrics to measure effectiveness? - Are there mechanisms to achieve independent assurance that information security is effectively managed? - Is there organisation-wide recognition of security accountability and responsibility?
Information security resource allocation	- Do you have a framework within which you can make investment decisions and determine the impact of cutting expenditure or curtailing projects? - Do you know how much you are spending and on what? - How do you measure your return on investment?
Know what is important to your business and the threats it might face **(Risk Assessment)**	- Have you identified and assessed the major threats to your business? - Do you know what would be the impact on the organisation if a serious security incident or loss of availability occurred, in terms of reputation, revenue, legal, operational performance and investor confidence?
Risk mitigation	- Have you done enough to identify and minimize the risks to your business operations? - Are the controls/safeguards robust enough to deal with a range of disasters? - Have you consider whether you have too much or not enough security to support your organisation - Have you considered what technological safeguards/controls could provide you with more effective security, whether in terms of cost, service, reliability ect. - Are your organisation's future needs taken into account when purchasing new technological safeguards/control measures?

(SOURCE: Ernst & Young "Global information security survey" (last visited 24 July 2002) http://www.ey.com/global 1-17).