

# **IT and Information Security Strategy 2009-2011**



Document Name	Information Security Strategy 2009-2011
Scope	Strategy plan for next three years
Security Analyst & Author	Firoz Haider Khan
Creation Date	25.06.2009
Reviewed By	
Review Date	
Approved by IT/ Technology Management Team	
Approved Date	
Version	1.0
Document Font	Times New Roman
Document Owner	Firoz Haider Khan , Head of Information Security , Securitysense Ltd.
Document Sponsor	
Document Type	Company CONFIDENTIAL

## Document Amendment Records

A =Added, M = Modified, D = Deleted

Version No.	Date	Section No.	A/M/D	Description of Change
Version 1.0				First Release.

## Table Of Contents

Chapter	code	Name of the Content	Page No
	I	Executive Summery	4
	II	Introduction	5
<b>Chapter - 1</b>		<b>Current and desired network architecture</b>	<b>6-9</b>
	1.0	Network architecture	6
	1.1	Current network architecture block diagram	6
	1.2	Desired network architecture block diagram	7
	1.3	Current network architecture schematic diagram	8
	1.4	Desired network architecture schematic diagram	9
<b>Chapter - 2</b>		<b>Current and desired state of information security</b>	<b>10-17</b>
	2.0	Functional area of information security	10
	2.1	Access control management	11
	2.2	Threat & Vulnerability Management	13
	2.3	Framework-Policy, Procedure and Guidelines	14
	2.4	Security Assessment and Monitoring	16
	2.5	Security Awareness and Education	17
<b>Chapter - 3</b>		<b>Information security strategy and initiatives</b>	<b>19-28</b>
	3.0	Information security strategy and initiatives in one page	19
	3.1	Strategy 1:Security Policy Enrichment and Maintenance	21
	3.2	Strategy 2: Information Security Risk Management	22
	3.3	Strategy 3: Development of security culture	23
	3.4	Strategy 4: Deploy Information Security technology solutions.	24
	3.5	Strategy 5: Incident Management and Computer Forensics	26
	3.6	Strategy 6: Information Security assessment	27
	3.7	Strategy 7: R & D of future security trends	28

## I. Executive Summary

Information security team is pleased to present the Information Security Strategic Plan for Securitysense for 2009-2011. Information Security planning is the process of determining how best the organization can use information asset to further its mission and tie system priorities to technology trends. This plan sets priorities for management, control, and protection of the Securitysense's information assets.

The planning document covers the next three (3) calendar years, 2009-2011 includes following 7 high-level strategic objectives with 46 initiatives ( see page # ) : and presents the primary goals, objectives, activities and critical success indicators of the information security ,Securitysense.

**# 1: Security Policy Enrichment and Maintenance:** complete enterprise security policy and standard framework

**# 2: Information Security Risk Management:** Proactive risk management

**# 3: Development of Security Culture:** training and education that will create an elevated awareness of the threats, vulnerabilities, and risk reduction techniques.

**# 4: Deploy Information Security Technology Solutions:** technology support secure common company business needs.

**# 5: Incident Management and Computer Forensics:** enterprise-wide approach to record, identify, and manage information security incidents

**# 6: Information Security Assessment:** evaluation of security posture and reveal weaknesses, vulnerabilities, threat contributing to overall risk.

**# 7: R & D of future security trends:** integrated approach that will further the integration of security while allowing sector experts to continue to advance best-of-breed resources.

Although covering a three year period, the Plan will be reviewed and updated through a continuous planning cycle as business needs change, and budgets and resources fluctuate. The goals, objectives and activities cited in this plan carry high expectations for new and exciting technological endeavors during the next three years.

Strong management commitment and support are crucial to the implementation of this plan. Successful implementation will ensure information is both protected and available, and that critical services are available when needed.

## II. Introduction

Information is life blood of any organization. Securitysense recognizes that information is a critical asset. How information is managed, controlled, and protected has a significant impact on the delivery of services and on the trust instilled in the users of those services. Information assets, including those held in trust, must be protected from unauthorized disclosure, theft, loss, destruction, and alteration. Information assets must be available when needed, particularly during emergencies and times of crisis.

The rapidly expanding use of the internet has increased the need for connectivity between SECURITYSENSE entities, third parties, and users of our offer services. This increase in connectivity has increased the SECURITYSENSE's risk posture and made it more difficult to protect information. Cyber crime has skyrocketed over the past few years, shifting from crimes of notoriety to far more serious crimes for financial gain. Attackers have become much more sophisticated in perpetrating and concealing cyber crimes, typically operating in stealth mode with a goal of avoiding detection altogether.

This document is company-wide information security strategic plan for the Securitysense. It sets priorities for how the company can efficiently and effectively address the management, control, and protection of information assets. It outlines the company's information security's three year vision, articulated as seven high-level Strategic Objectives followed with 46 initiatives.

There are significant gaps between where the company's information security is today and the three year vision. The importance of the strategic objectives was assessed, prioritizing the gaps. The results of this assessment are summarized as **Key Initiatives**; a three year strategic plan. A set of business and tactical plans detailing the deliverables necessary to achieve the key initiatives are maintained separately.

Securitysense leaders and cross functional securities responsible are the primary audience of this plan. From an information security perspective, they need to know the current state, the future vision, and the task necessary to bridge the gap. Achieving the strategic objectives will not be possible without strong management commitment. SECURITYSENSE leaders and management must understand and have confidence in this plan.

Finally, SECURITYSENSE employee, business partners and subscribers, – the end users of Securitysense services – have a vested interest in the success of this plan. End users of SECURITYSENSE services need to have complete confidence that SECURITYSENSE entities will protect their data from unauthorized disclosure. End users must be confident

that critical SECURITYSENSE services will be available when needed, particularly during times of crisis.

## CHAPTER: 1

### Current and desired Network Architecture

#### 1.0 Current and desired Network Architecture status

Securitysense has implemented several protection mechanism/devices to secure the network from any unauthorized / hacking activities. Internet firewall, IDS, CDN & content firewall, remote access through VPN etc. are already in place in the current network architecture. But security is a continual cycle and hence need to be always updated with the latest technologies. To create a standard secure environment, some additional implementations are required such as improved network segregation for critical servers, internal firewall protection to these critical servers, intrusion protection system implementation instead of intrusion detection system, identity management systems and all remote connection through VPN and two factor authentication etc. All of these have been summarized in the bellow mentioned current and desired network architecture block and schematic diagram

#### 1.1 Current network architecture block diagram:

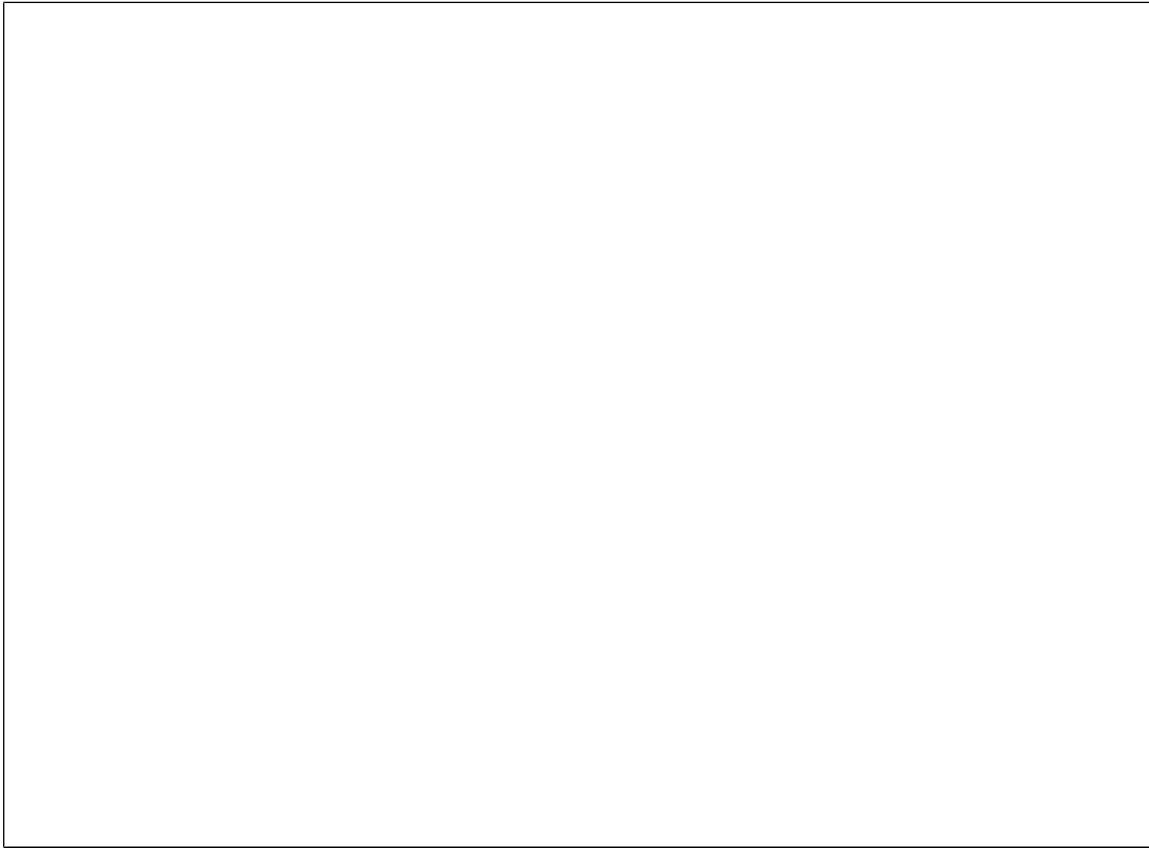


Figure: Current Network Architecture Block Diagram

**1.2 Desired network architecture block diagram:**

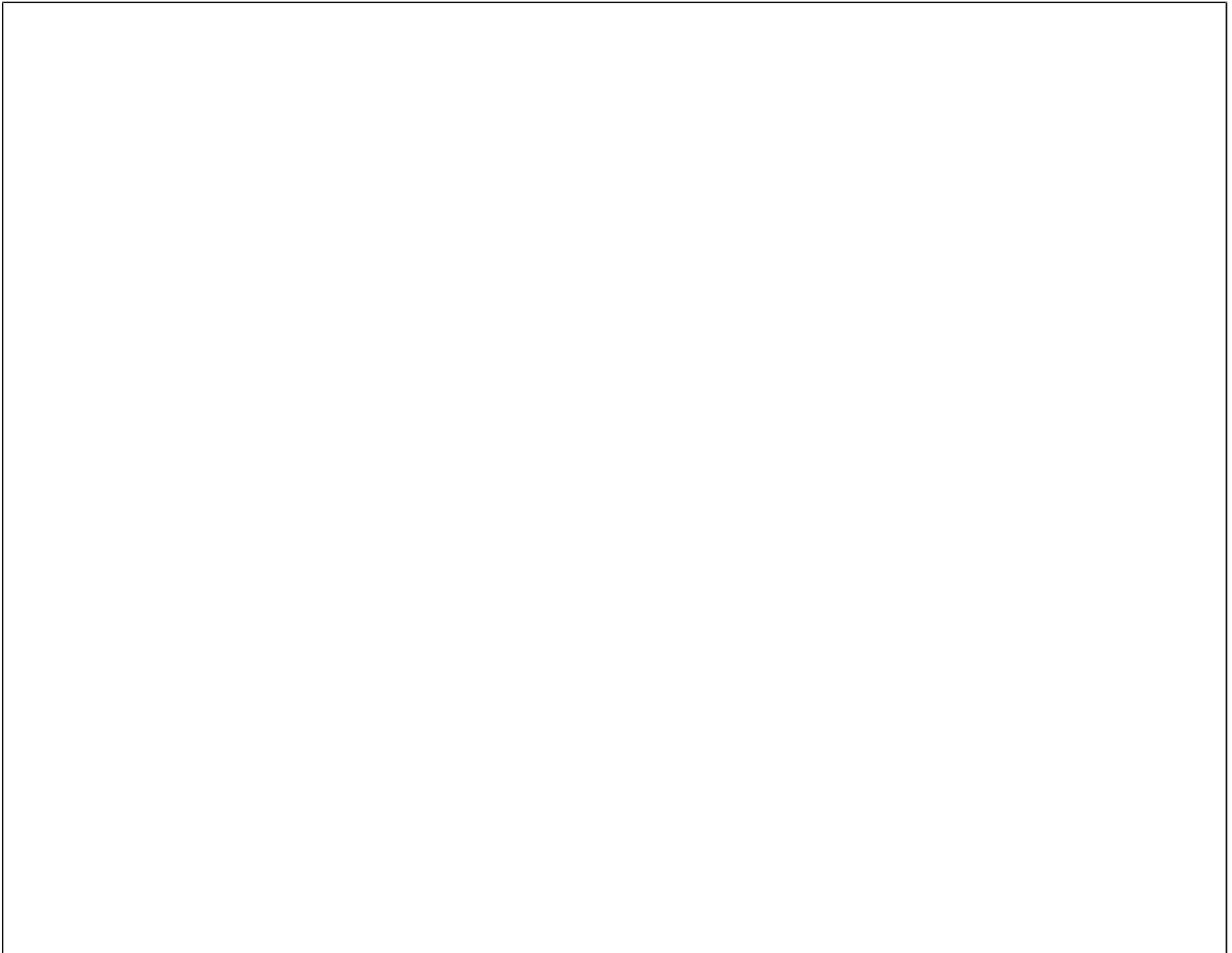


Figure: Desired Network Architecture Block Diagram



### 1.3 Current network architecture schematic diagram:

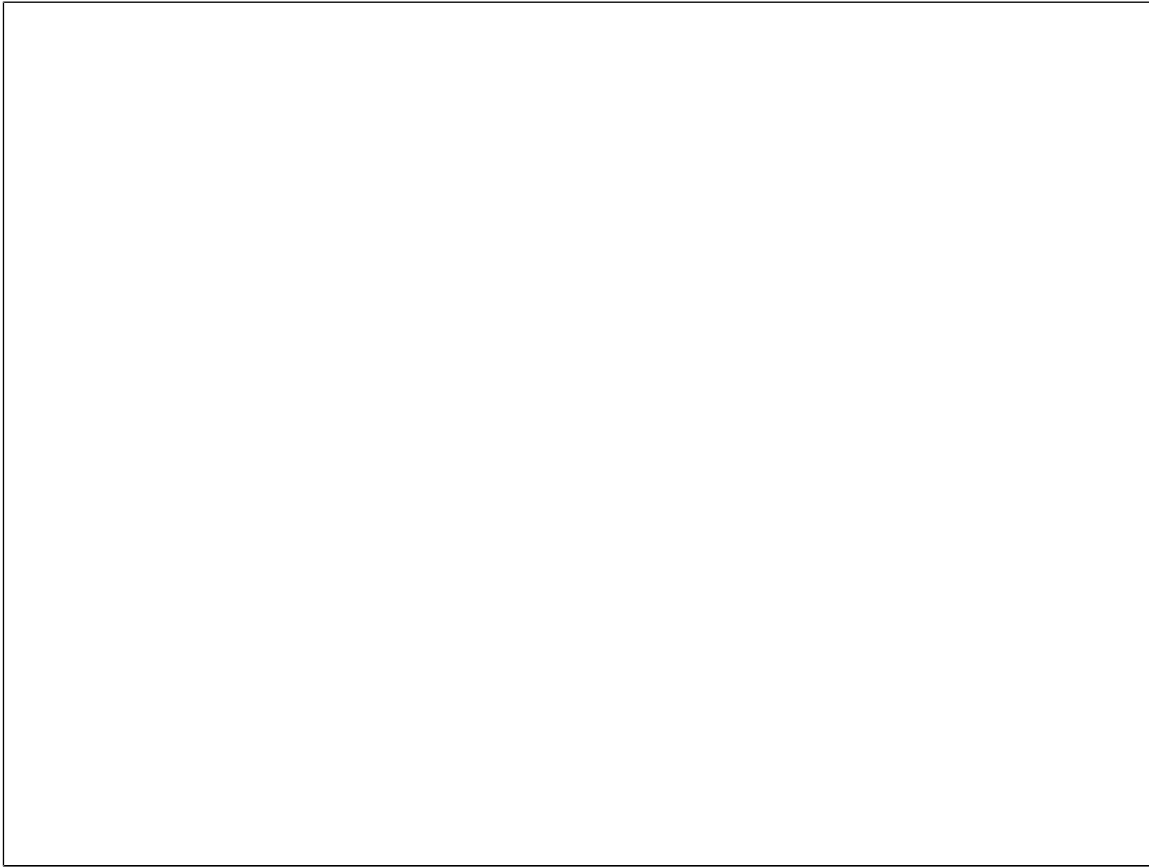


Figure: Current Network Architecture Schematic Diagram

#### 1.4 Desired network architecture schematic diagram:



Figure: Desired Network Architecture Schematic Diagram

## CHAPTER: 2

### Current & Desired State of Information Security

#### 2.0 Information Security Functional area

The "spider diagram" (Figure: 1) shows the five security functional areas (SFAs) that make up the security environment of Securitysense. To evaluate the current state of the environment, we have rated the level of security in each area, on a scale of 1 to 5 .

5= Excellent or optimized, 4= Very Good, 3= Good, 2= Poor, 1= Very poor ( just started or not integrated )

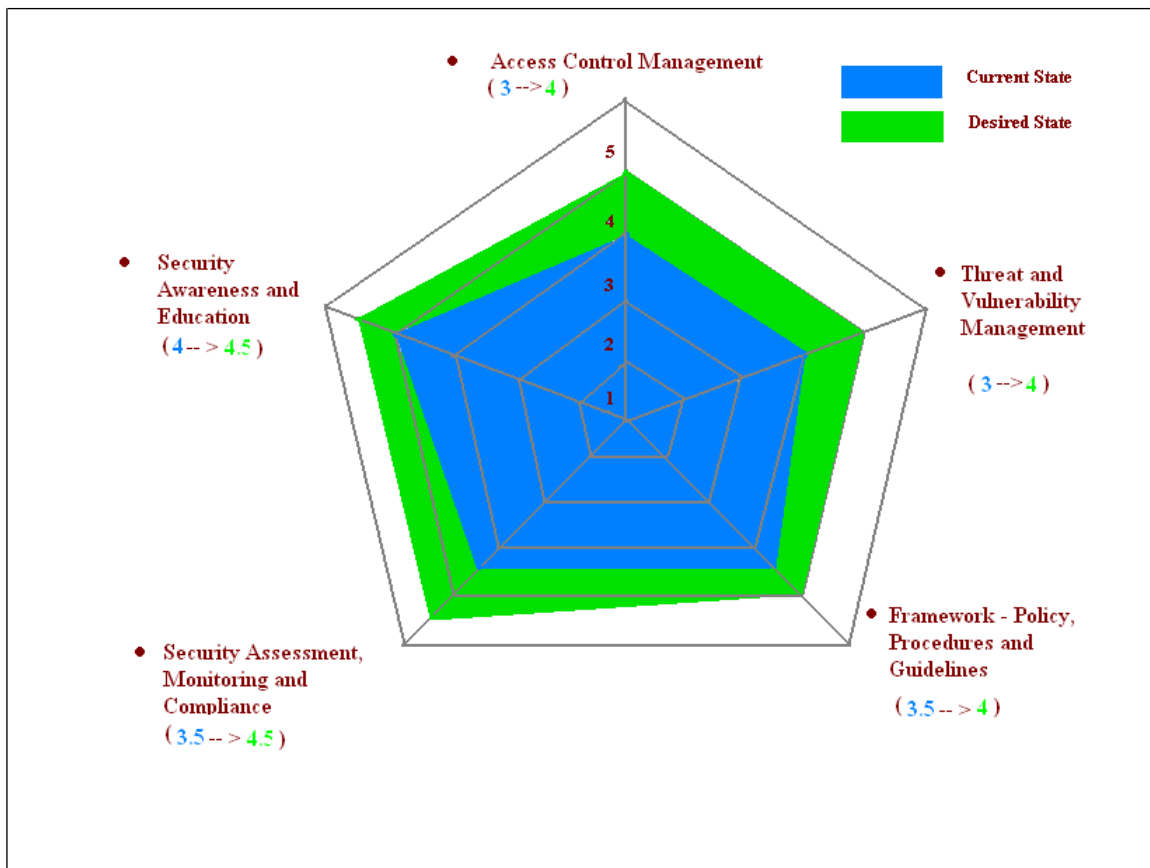


Figure: Current and Desired State of security

## 2.1 Access Control Management

Criteria	Current status	Rating
Access control policy	Excellent (Optimized)	3
Centralized user access control in various systems	Very Poor (Just started or not integrated)	
Security tools implemented in the network	Good	
Remote users access control	Good	
Effective firewall implementation to protect hackers	Good	

### Current State of Security: Access Control Management

Decentralized access management system is in practice in Securitysense. Access control mechanism and control are built in separately in different application, OS, database and systems. This decentralized system is not capable of monitoring all users' access permission and activities from a central location. The following control, tools are in place for secure access management:

- Windows domain controller to authenticate internal users and controls a variety of file & exchange server permissions.
- Access control policy exists and revision is done yearly.
- Remote user's connectivity to internal networks and systems through VPN, https and SECURITYSENSE RS connection.
- TACACS+ authentication system for fist level authentication of VPN and Webmail access.
- Centralized logging for CDN systems where RSA two factor authentication is implemented.
- IT and CDN Firewall to protect any unauthorized access and ensure a hacker free SECURITYSENSE network infrastructure.
- SSL certificate server to secure the web service connectivity.
- Website access restriction mechanism through the use of proxy server for internet connection.

### Desired State of Security: Access Control Management

Centralize and automate secure identity-related processes are required to support the identity lifecycle across every IT system, manage IT security risk and improve

compliance. Following tools and technologies can add value to reach desired state of access control management functional area:

- **Identity Management Solutions** should be in place to achieve the purpose of centralized access control. It allows managing end-to-end lifecycle of user identities across all enterprise resources.
- **Network Access Control (NAC)** system should be implemented which will control access to a network with policies, including pre-admission endpoint security policy checks and post-admission controls over where users and devices can go on a network and what they can do. Guest users can also be controlled with this implementation.
- **Password sharing** is practiced among the system administrators which must be controlled to protect any breach of security at server level.
- Document **Rights Management System (RMS)** should be implemented to protect and control usage of the document where owner can decide the modification, printing, and other privileges to users.
- **Automated Configuration Management and Assessment** Server is recommended to have some central provisioning of device configurations and security policies for security devices such as internal and external firewall, VPN concentrator (and Intrusion detection or prevention Systems (IDS /IPS). This can be achieved through intelligent policy-based management techniques that can simplify administration and deliver comprehensive policy administration and enforcement.
- **Mobile device control and encryption** tools should be implemented. It will protect the use of unauthorized USB drives, hard drives or any other removable devices. It will also reduce the probability of infection internal systems by malicious codes and protect disclosing internal information of Securitysense to outside world.
- All the users to go through the proxy server with proper URL filtering. Any user required doing VPN connectivity to Telenor or any other network can have a filtering rule on the firewalls allowing access on the port designated for the protocol used for VPN tunneling. If DHCP is used then an IP can be permanently leased to the user for on which the rule on the firewalls would be set.

- Implementation of **two-factor authentication** (such as hardware tokens) with VPN client – server communication is recommended for all remote users. No user should be allowed to access remotely without these in place. Also the use of such two-factor authentication systems is recommended for access to critical server by system owners or administrators.
- It requires binding user access with only permitted VPN Group remotely. Currently a TACACS authentication permitted user can connect through any VPN group if he/she has the VPN group password.
- Changes in the VPN concentrator deployment design are required. Presently the traffic passes through VPN concentrator does not pass through firewall and no access restrictions are applied.

## 2.2. Threat & Vulnerability Management

### Current State of Security: Threat and Vulnerability Management

Criteria	Current status	Rating
Detection mechanism implemented	Good	3
Protection mechanism implemented	Good	
Proactive Threat and Vulnerability management	Good	
Patch management system	Very good	

Manual threat and vulnerability management system is in practice in Securitysense. A security breach can cost a company millions of dollars and have a tremendous negative impact on the company's public image and customer trust. These manual processes can not always protect spreading of infection throughout the network. Besides, vulnerabilities can not be detected on real time basis. The following control, tools are in place for ensuring threat and vulnerability management:

- An Intrusion Detection System (IDS) is placed in the network to detect any attempt of intrusion which is being controlled and monitored by Telenor. Telenor security operations centre inform SECURITYSENSE responsible team if any intrusion is detected and thereby SECURITYSENSE internal team perform actions to protect/cure the intrusion.
- Monthly vulnerability scan is performed for IT server VLAN to find out the status of the servers in respect of current world vulnerability exposure. The

scanning result is being analyzed and shared with relevant systems owners/administrators to cure the systems from relevant threats.

- Antivirus control is implemented throughout the organization to protect systems, nodes from virus, worm, Trojan horse, spyware or any other malicious code attack on real time basis. The signature file of the antivirus is updated automatically checking the status of update server.
- Spam and content filter for email flow is physically present in Telenor to scan all external incoming emails to the SMTP server
- Reverse proxy server has been integrated with the existing network which protects any direct exposure of business related front end web server to internet. The communication through these servers is on https connection thereby encrypting data from end user to server which protect any chance of hijacking established session to the servers.

### **Desired State of Security: Threat and Vulnerability Management**

Automated threat and vulnerability management system is required to protect internal business systems and services from any attack or hacking attempt from unauthorized users and sources. Following tools and technologies can help to reach desired state of threat and vulnerability management functional area:

- Network based **IPS sensors** along with host based IPS sensors within all critical business application servers should be implemented. The product selected should be able to be seamlessly inserted and transparently into the network. As packets pass through the IPS, they are fully inspected to determine whether they are legitimate or malicious. If any malicious packet found will be eliminated or quarantined and based on the policy an alarm would be generated to the relevant source.
- An **Internal Firewall** should be implemented segregating the entire internal mission critical server from the user VLANs. It will also ensure the security of the critical systems in case of any mishap of the Internet firewall.
- **Automated Vulnerability and Risk Management** tools to be used in SECURITYSENSE which would help SECURITYSENSE to schedule scans proactively based on some policy sets. After scanning a proper threat score analysis would be carried out which would help SECURITYSENSE to calculate and understand their current risk posture of the network.
- Modification of VPN concentrator deployment and Internet configuration to disable ICMP on the VPN concentrator thus protecting the VPN concentrator against DOS attacks.

- The front-end exchange server should be placed in the DMZ properly segregated from the other mail servers with adequate content and spam filter mechanism.

## 2.3 Framework-Policy, Procedure and Guidelines

### Current State of Security: Framework-Policy, Procedure and Guidelines

Criteria	Current status	Rating
Does security framework exist?	Very Good	3.5
Do policies cover all area?	Very Good	
Review frequency of policies	Good	
Effective policy deployment status in field level	Good	

To ensure complete security of organizational assets, policy, procedure and guidelines play the most important role. In fact, these are the commitment and direction of management whose main purpose is to inform users, staff, and managers of their obligatory requirements for protecting technology and information assets. Framework of Information Security already exists in current practice. Besides, the following policy, procedure and guidelines are implemented in Securitysense to secure the systems as well as organization:

- Access control policy
- Access control policy & procedure
- Backup and Recovery Procedure
- Incident Handling procedure
- Email distribution policy
- General & Miscellaneous rules
- General Rules for Information Access Rights
- Information Classification Policy
- Information protection policy



- Information Security Incident Handling Procedure
- IT Policy-Procedure and Review Frequency
- Local Procedure Information Security
- Media Disposal Policy
- Remote access policy
- Router Security Policy
- Router security Policy Appendix
- Rules for End-user Password and Privileges
- Rules for Internet use
- Rules for using File Server storage
- Rules for using SECURITYSENSE PABX
- Segregation of Duties
- Standard software and hardware
- Virtual Private Network (VPN) Policy
- Wireless Communication Policy

### **Desired State of Security: Framework-Policy, Procedure and Guidelines**

Development of a complete set of policy, procedure and guidelines ensures the security of an organization from all aspects. These policies are the strategic aims and control objectives that guide the development of organizational information security management systems. Lacking of any critical policy creates a security threat for the whole organization. Following initiatives and improvements can contribute to reach desired state of Framework-policy, procedure and guidelines functional area:

- Information security control should be incorporated in System development life cycle (SDLC) and its effective usage needs to be ensured in all implementation.
- A general guideline for project development should be incorporated. It will help the project managers to ensure all the security requirements in every deployment of OS, application and services.

- Standard Review of Information Security policies in every year to assure consistency, minimization of duplication, and compliance with security standards.
- Information security risk management methodology and policy should be developed.
- Information Security incident reporting systems should be streamlined.
- Log management policy for various systems should be developed.

## 2.4 Security Assessment, Monitoring and Compliance

### Current State of Security: Security Assessment, Monitoring and Compliance

Criteria	Current status	Rating
Security assessment / audit frequency	Very Good	3.5
Internal assessment / audit	Very Good	
External(ISO, SOX, Third Party) assessment / audit	Very Good	
Compliance with ISO 27001, SOX, COBIT, Telenor SECURITYSENSEI and Local Framework	Very Good	
Security control deployment based on assessment/audit report	Good	
Centralized logging for business critical systems	Very poor (Just started or not integrated)	
Log analysis and security reporting	Good	

Security assessment & monitoring arrangement provides key decision with an informed view of the effectiveness and efficiency of information security arrangements and the area where improvement is required.

Regular assessment of security and monitoring is essential to streamline the security implementation which is a continuous process. The following security assessment and monitoring measures are pursued in Securitysense to secure the systems as well as organization:

- Information Security team reviews company security policies and procedures yearly.
- Group Risk Team Security from Telenor also perform audit on yearly basis.
- Internal control team of Securitysense conduct audit on quarterly basis to ensure systems security which is part of SOX.

- Internal audit team of Securitysense audits the security control to ensure compliance.
- Logs of IT firewall from log analyzer, antivirus and IDS are analyzed every month to evaluate the unauthorized access attempt, attack trend and existing controls implemented to protect these attempts.
- SECURITYSENSE's policy or standard conformed to International Standards and Guidelines like ISO 27001, SOX, COBIT, ICT Act.

### **Desired State of Security: Security Assessment, Monitoring and Compliance**

External security assessment and proactive monitoring of activities in the network will assist ensuring proper security of our systems. Following initiatives and improvements can contribute to reach desired state of security assessment, monitoring and compliance functional area:

- External third party security assessment and implementation of recommended measure to mitigate the risk to secure the organization.
- Penetration test from information security at regular interval to assess the existing security of network and suggest relevant system administrators if any weakness is discovered.
- A centralized security information management and logging system for all business critical systems, OS, database should be implemented so that the status of security and threat can be evaluate on real time basis.
- Team should work together for the improvement so that compliance with international standards becomes more aligned.
- Grameen phone should be an ISO 27001 certified company.

## **2.5 Security Awareness and Education**

### **Current State of Security: Security Awareness and Education**

<b>Criteria</b>	<b>Current status</b>	<b>Rating</b>
Does awareness program cover all employees?	Very Good	4
Communication method of awareness	Very Good	
Does Training program meet basic security information?	Excellent	
Quality of program	Very Good	
Frequency of Awareness program	Very Good	

Employee (user) should be made aware of the key elements of the information security and why it is needed and understand their personal security responsibilities.

Security awareness and educational program are essential to enhance employee knowledge about information security. These programs help to understand every employee roles and responsibility as they relate to basic practices for information security. Overall, security is everyone's responsibility. The following security awareness and educational measures are taken in Securitysense:

- Information security team regularly organizes awareness program.
- Information security team also takes initiatives to aware all employees through monthly email, desktop wallpaper, banner, poster and sticker.
- Trainings are arranged in need basis for System, Network, Database, and Application administrator, analyst by internal or external experts.
- Evaluation of awareness and training program is performed to ensure the effectiveness of the program.

#### **Desired State of Security: Security Awareness and Education**

Regular and interactive security awareness and education will enhance information security related knowledge as well as world trend of best practice in this filed. The following initiatives can be taken to reach the desired state of security awareness and education functional area:

- Information security awareness program should be arranged in such a way that it touches each and every employee of Securitysense.
- Organizing Security training and education for administrator (System, Network, Database, application administrator, analyst) on regular basis not in need basis.
- A Central awareness and training program arrangement solution should be developed so that a single program can cover many purposes reducing expenses and other difficulties.
- An Information Security Web portal and Blog can be developed for better understanding of security knowledge.

## CHAPTER: 3

### Information security strategy and initiatives

#### 3.0 Information security strategy and initiatives at a glance

Information Security Strategy (2009, 2010, 2011)	
Strategy	Initiatives
1. <i>Security Policy Enrichment and Maintenance</i>	<ol style="list-style-type: none"> <li>1. Develop additional targeted policies and procedures</li> <li>2. Review Information Security policies to assure consistency, minimization of duplication, and compliance with security standards.</li> </ol>
2. <i>Information Security Risk Management</i>	<ol style="list-style-type: none"> <li>1. Develop risk assessment methodology</li> <li>2. Identify information asset and set CIA values (Confidentiality, Integrity and Availability).</li> <li>3. Identify existing threats and vulnerabilities</li> <li>4. Conduct information risk assessment.</li> <li>5. Determine a risk mitigation strategy based upon cost-benefit analysis</li> <li>6. Perform mitigation activities</li> </ol>
3. <i>Development of security culture</i>	<ol style="list-style-type: none"> <li>1. Security Awareness program Enhancement</li> <li>2. Security training and education for administrator (System, Network, Database, application administrator, analyst)</li> <li>3. Security awareness assessment</li> <li>4. Information Security Web portal and Blog</li> </ol>
4. <i>Deploy Information Security technology solutions.</i>	<ol style="list-style-type: none"> <li>1. Deploy Identity Access Management.</li> <li>2. Integrate Windows Right Management System (RMS)</li> <li>3. Introduce Mobile device control and encryption tools</li> <li>4. Implement Network Access Control (NAC) for internal network.</li> <li>5. Deployment of Internet content filtering mechanism for SECURITYSENSERS users.</li> <li>6. Incorporate information security control in SDLC.</li> <li>7. Develop information security Guideline for project management.</li> <li>8. Enhance effective monitoring and protection against malicious code (virus, spyware, phishing, worm etc).</li> <li>9. Enhancing VPN concentrator (replacement) protection and VPN access mechanism.</li> <li>10. Segregation of networks for business critical servers.</li> <li>11. Internal firewall implementation to increase the security of mission critical servers.</li> <li>12. Implementation of network and host based Intrusion Protection System (IPS).</li> </ol>

	<ol style="list-style-type: none"> <li>13. Establishing Front-end Exchange server in DMZ with adequate content and spam filtering mechanism.</li> <li>14. Implementation of central logging server.</li> <li>15. Implementation of two-factor authentication system for all remote access</li> <li>16. Development of test environment guideline.</li> <li>17. Development of hardening guideline for OS, Application, Databases and Security systems.</li> <li>18. Implementation of SECURITYSENSE traffic monitoring system (Lawful Interception).</li> <li>19. Developing a web hosting platform to ensure security and protection of the web services provided to customers.</li> <li>20. End point security (for Exchange 2007: Forefront V.10) for multi-layered protection, file filtering, premium anti-spam protection, centralized reporting, notifications and alerts.</li> <li>21. Integrated EGDE security Gateway for Windows applications (ISA 2006) to defend against external and internal threat as well as publish application link using a security gateway to access inside.</li> <li>22. End to End service Management Solution (for Performance Monitoring, Patch deployment, MS Software Delivery etc.).</li> <li>23. TACACS Server version up-gradation to implement better protection features.</li> <li>24. Restructuring IT Firewall DMZ zone to implement robust zonal concept appropriately.</li> <li>25. Implementation of share account and privilege account management tools.</li> </ol>
5. Incident Management and Computer Forensics	<ol style="list-style-type: none"> <li>1. Streamline information Security Incident report system</li> <li>2. Increase suite of forensics tools to measure internal network security strength.</li> <li>3. Scanning network node.</li> </ol>
6. Information Security assessment	<ol style="list-style-type: none"> <li>1. Conduct third party information security audits in SECURITYSENSE.</li> <li>2. Be a ISO 27001 certified company</li> <li>3. Security control remediation activities in support of compliance requirements such as the Sarbanes-Oxley Act.</li> </ol>
7. R & D of future security trends	<ol style="list-style-type: none"> <li>1. Setup a information security lab</li> <li>2. Participate international information security workshop/conference</li> <li>3. Relationship development with local security concern authorities and institute.</li> </ol>

**Total 46 Initiatives in 7 strategies.**

### 3.1 Security Policy Enrichment and Maintenance

#### ***Strategy 1: Security Policy Enrichment and Maintenance***

##### **Brief Description:**

The first and most important underlying objective of company information security approach is the development and maintenance of policies, standards and procedures to identify the company's security requirements. This will assist staff in implementing the appropriate controls to protect sensitive information for which they are responsible.

This document should state management commitment and set out the organization's approach to managing information security.

##### **Objectives:**

- A companywide approach to information security.
- Prevent the compromise and the misuse of company's information.
- Protect the reputation of the company and satisfy its legal and ethical responsibilities.

<b>Initiatives</b>	<b>Responsible</b>	<b>Time</b>
<ol style="list-style-type: none"> <li>1. Develop additional targeted policies and procedures</li> <li>2. Review Information Security policies to assure consistency, minimization of duplication, and compliance with security standards.</li> </ol>		

## **3.2 Information Security Risk Management**



## ***Strategy 2: Information Security Risk Management***

### **Brief Description:**

In today's environment, there are numerous threats to the confidentiality, integrity, and availability of Information Technology systems and the data that reside on them.

Information risk is the chance or possibility of harm being caused to a business as a result of a loss of the confidentiality, integrity or availability of information. A process approach for assessing risks, treating risks and ongoing risk monitoring, risk reviews and re-assessments plans shall be documented.

The risk assessment process shall cover a selection of processes and systems for assessment. The risk assessment process for information systems shall take system class into consideration. These include solutions that ensure systems connecting to the SECURITYSENSE's network are properly configured, that ensure vulnerabilities are being identified and remediate in an efficient manner and that minimize the potential impact of a security compromise

### **Objectives:**

- Develop methodology of risk assessment
- Information Assess Classification
- Reduce Risk and Vulnerability

<b>Initiatives</b>	<b>Responsible</b>	<b>Time</b>
<ol style="list-style-type: none"> <li>1. Develop risk assessment methodology</li> <li>2. Identify information asset and set CIA values (Confidentiality, Integrity, and Availability).</li> <li>3. Identify existing threats and vulnerabilities</li> <li>4. Conduct information risk assessment.</li> <li>5. Determine a risk mitigation strategy based upon cost-benefit analysis</li> <li>6. Perform mitigation activities</li> </ol>		

### **3.3 Development of security culture**

### ***Strategy 3: Development of security culture***

#### **Brief Description:**

Employees are often the weakest links in securing systems. Even the best technological and physical controls can be defeated easily if the human factor is weak. It is imperative that all employees be part of the human defense posture maintained by the company.

This can only be accomplished through proper training and education that will create an elevated awareness of the threats, vulnerabilities, and risk reduction techniques.

Security education, training, and awareness program shall be in place to ensure related resources and end-users are aware of the security issues and their implications. Employee (user) should be made aware of the key elements of the information security and why it is needed and understand their personal security responsibilities.

#### **Objectives**


- Raise Awareness
- Enhance Staff Skills

<b>Initiatives</b>	<b>Responsible</b>	<b>Time</b>
<ol style="list-style-type: none"> <li>1. Security Awareness program Enhancement</li> <li>2. Security training and education for administrator (System, Network, Database, application administrator, analyst)</li> <li>3. Security awareness assessment</li> <li>4. Information Security Web portal and Blog</li> </ol>		

### **3.4 Deploy Information Security technology solutions.**

## Strategy 4: Deploy Information Security technology solutions.

### Brief Description:

Deploy Information Security technology solutions are important in support secure common company business needs. Technology resources like IDM, RMS,  SecuritySensors required in the reduction of vulnerability are finite, so these resources should be allocated first to the vulnerabilities associated with highest value targets.

### Objectives

- Ensure Confidentiality, Integrity & Availability of information asset.
- Identify and protect complex cyber attacks
- Reduced time and cost to investigate security incidents
- Consistent and robust monitoring of all security incident
- Centralized Identity and Access Control Management

Initiatives	Responsible	Time
<ol style="list-style-type: none"><li>1. Deploy Identity Access Management.</li><li>2. Integrate Windows Right Management System (RMS)</li><li>3. Introduce Mobile device control and encryption tools</li><li>4. Implement Network Access Control (NAC) for internal network.</li><li>5. Deploy Internet content filter for SECURITYSENSORS users.</li><li>6. Incorporate information security control in SDLC.</li><li>7. Develop information security Guideline for project management.</li><li>8. Enhance effective monitoring and protection against malicious code (virus, spyware, phishing, worm etc )</li><li>9. Enhancing VPN concentrator (replacement) protection and VPN access mechanism.</li><li>10. Segregation of networks for business critical servers.</li><li>11. Internal firewall implementation to increase the security of mission critical servers.</li><li>12. Implementation of network and host based Intrusion Protection System (IPS).</li><li>13. Establishing Front-end Exchange server in DMZ with adequate content and spam filtering mechanism.</li><li>14. Implementation of central logging server.</li><li>15. Implementation of two-factor authentication system for all remote access</li><li>16. Development of test environment guideline.</li><li>17. Development of hardening guideline for OS, Application, Databases and Security systems.</li><li>18. Implementation of</li></ol>		

### 3.5 Incident Management and Computer Forensics

#### ***Strategy 5: Incident Management and Computer Forensics***

##### **Brief Description:**

Securitysense will maintain a Security Incident management procedure to ensure that Information Security events and weaknesses associated with Information processing facilities are communicated in a manner allowing timely corrective action to be taken. Documents shall be in place to ensure that any significant event is reported, logged and collected for analysis. Procedures shall assure incident investigations are complete and minimize further damage. Information Security will create and maintain policies, standards, and procedures to institutionalize the elements of Incident Management.

Computer forensics capabilities are required to determine what has transpired in our systems at a user level, or on a system level, after the fact. This could be to investigate computer abuse, an automated malware infestation or attack, or a targeted attack against any system. Forensics tools are also needed by our investigative and law enforcement partners, and we endeavor to make our facilities, resources, and skills useful and available to them.

##### **Objectives**

- Company-wide approach to record, identify, and manage information security incident
- Conduct penetration & hardening test to identify security loopholes of all information assets

<b>Initiatives</b>	<b>Responsible</b>	<b>Time</b>
<ol style="list-style-type: none"> <li>1. Streamline information Security Incident report system</li> <li>2. Increase suite of forensics tools to measure internal network security strength.</li> <li>3. Scanning network node.</li> </ol>		

### 3.6 Information Security assessment

<b>Strategy 6: Information Security assessment</b>		
<p><b>Brief Description:</b>            An assessment is generally performed to obtain an objective evaluation of security posture and reveal weaknesses, vulnerabilities, threat contributing to overall risk.            Information security - Securitysense will conduct a third party review annually to check the objectives and controls set by Information Security Procedure are properly carried out.</p>		
<p><b>Objectives</b></p> <ul style="list-style-type: none"> <li>• Ensure organization's information, information technology and business systems are adequately controlled, monitored and assessed.</li> <li>• Evaluation organization's security status.</li> <li>• Set auditable specification where it requires.</li> <li>• Increase company reputation and brand image.</li> </ul>		
<b>Initiatives</b>	<b>Responsibility</b>	<b>Time</b>
<ol style="list-style-type: none"> <li>1. Conduct third party information security audits in SECURITYSENSE.</li> <li>2. Be a ISO 27001 certified company</li> <li>3. Security control remediation activities in support of compliance requirements such as the Sarbanes-Oxley Act.</li> </ol>		

### 3.7 R & D of future security trends

#### ***Strategy 7: R & D of future security trends***

##### **Brief Description:**

Multi-pronged security threats posed by new technology combinations require a new, integrated approach that will further the integration of security while allowing sector experts to continue to advance best-of-breed resources.

Security professional should seek skills that will work together to combine strengths, intelligently identify new complex threats, and to move information efficiently through personalized parameters made possible through knowledge share and other new technologies.

##### **Objectives**

- Confidence and competent development for information security professional
- Proactive alignment with future security control
- Pilot deployment of upcoming security tool

<b>Initiatives</b>	<b>Responsibility</b>	<b>Time</b>
<ol style="list-style-type: none"> <li>1. Setup an information security lab.</li> <li>2. Participation in international information security workshop/conference.</li> <li>3. Relationship development with local security concern authorities and institute.</li> </ol>		