Version Control

Owner : Frode Stoldal, CTO **Author** : Firoz Haider Khan **Revised by** : BCM Program Manager **Approved by** : MT **Current Version** : v1.0	**Revised Date** : Jan 09 **Approval Date** : 24 Feb 09 **Effective Date** : 1 Mar 09
File location:	**File Name :** Securitysense BC Policy.doc

Revision History

Sl.	Revision Number	Description	Approved By	Approved Date	Author / Prepared
1	1	Securitysense BC Policy	MT	24 Feb 2009	Lutfor Rahman Firoz H. Khan

Introduction

Business continuity is defined as ensuring the continuity or uninterrupted provision of operations and services. It ensure the availability of services, programs, and operations, including all resources involved, and the timely resumption of services in the event of a major failure, emergency or disaster.

Securitysense shall have the ability to ensure continuity and availability of service and support for customers, partners and the general public interest before, during and after a Crisis. Securitysense shall be prepared for critical emergency situations and trained for Business Continuity Management.

This policy sets out top management's direction on, and commitment to, Business Continuity. It defines the business continuity, staff responsibilities regarding business continuity and sets out the desired business continuity behavior for staff.

This is an ongoing process with several different but complementary elements, including disaster recovery, business recovery, business resumption, contingency planning, and crisis management.

_

Objective

- develop business continuity management programs to support Securitysense business objectives and continued delivery of essential services during a business interruption

- protect critical Securitysense infrastructure and assets necessary to sustain business continuity
- provide direction for management to prepare company-wide business continuity plans, and pre-position personnel and resources to mitigate the effect of a business interruption
- support Securitysense-wide emergency preparedness and response plans
- establish Securitysense-wide guidelines for the identification, analysis and treatment of potential business continuity risks to Securitysense services, programs or operations
- develop a Securitysense Business Continuity (BC) / Crisis Management (CM)Plan to support delivery of essential Securitysense services and continuous functioning of Securitysense during a major business interruption
- regularly monitor overall readiness, exercise completion, and audit of business continuity plans and reporting to the CEO on the status of Securitysense-wide Business Continuity Management Programs
- continuously promote Securitysense-wide business continuity processes, best practices, training and awareness for employees

Scope

This policy shall apply to Securitysense including the regional offices Chittagong, Rajshahi, Shylet, Khulna, Mymenshing, and Dhaka offices, jointly owned facilities, all other Securitysense-owned property, Securitysense-leased space, and temporary field operations and field trips that are under the control of Securitysense operations and staff.

Policy

1. Securitysense must manage Business Continuity Management (BCM) program across the company, in accordance with the ISO business continuity standards and guidelines.

2. Securitysense must conduct an annual strategic risk analysis of business objectives to identify business, program, and operational risks that could be impacted by a business interruption, and apply cost-effective risk mitigation treatments.
3. Securitysense must complete a comprehensive company-wide business impact analysis (BIA) annually, as well as when significant program changes occur, to identify and develop strategies to reduce the likelihood and consequence of a business interruption.
4. Securitysense BCM office must use the results of the risk analysis and business impact analysis to develop a priority-ranking of essential services, programs or operations, and develop appropriate risk mitigation strategies.
5. Securitysense must identify internal and external dependencies involved in the delivery of Securitysense services and develop mutually supportive business continuity strategies and establish contact point with local regulatory authority and law enforcing agency.
6. Securitysense must develop business continuity / Crisis Management plans and procedures to support Securitysense business objectives and availability of essential services. Plans must include:

- specific security plans and procedures to move up to heightened security levels in the event of an emergency or increased threat condition; and
- current lists of key resources required for the recovery and resumption of essential services. Resources include personnel, facilities, critical infrastructure and assets, information, materials and office equipment/furniture, information technology assets (hardware and software) and communications.

7. Securitysense must establish the capability to resume essential services by putting appropriate risk mitigation treatments in place to prevent and mitigate the effect of business interruption and support the timely recovery of business activities.
8. Securitysense shall ensure business survivability and continuity through Crisis situations. BC Plan must be link to Crisis Management Plan. Securitysense shall be ready to perform and/or provide clearly defined services to support Crisis Management when required
9. Securitysense must be exercised Business continuity / CM plans at least annually to the extent necessary to confirm plan effectiveness and to ensure personnel are prepared and trained. Every Second year the BCM office shall perform a functional exercise of local Business Continuity / Crisis Management plan,
10. Securitysense BCM office must coordinate business continuity/ CM plans with Information & Physical security management.
11. Securitysense BCM Office / ensure BC/CM documents are readily accessible during a business interruption or crisis. All employees and key stakeholders must be aware of the business continuity management program and understand its contents and their role.

Responsibilities and Implementation

CEO is responsible for safeguarding of Securitysense assets. CEO will assign a BCM Program Manager responsible for development and implementation of Business Continuity Program/ procedure in Securitysense. He /She is responsible for maintenance, implementation and monitoring of this procedure.

Each divisional/departmental / relevant cross functional team and employee is responsible for the operational continuity in their respective area. They are entitled to receive guidance and direction from BCM program Manger / BC Management as part of a cooperative effort for planning.

All planning will greatly rely on the input from the staff and faculty of each department to ensure a proper level of consideration is given to all aspects of that unit's critical functional operations

Document / Records Control & Review

The Securitysense BCM office will review BC policy, and relevant documents (BC, CM plan) annually to ensure they are current, valid and readily accessible during a business interruption. or any time if business need.

Business Continuity procedure/ relevant document shall be implemented and maintained. This document should state management commitment and set out the organization's approach to managing Business Continuity Program. All policy/procedure documents (BC Policy, BC Plan, CMT Plan etc) must be signed by CEO, Securitysense and should contain statements concerning

a. Approve documents for adequacy prior to issue.
b. Review and update documents yearly or as necessary';
c. Ensure that changes and the current version status of documents are identified.
d. Ensure that documents are available to those who need them.
e. Ensure that the distribution of documents is control;
d. Prevent the unintended use of obsolete documents

BC/ CM Records shall be established, maintained and controlled to provide evidence of the effective operation of the BCM. The controls needed for the identification, storage, protection, retrieval, retention time and disposition of records shall be documented. A management process shall determine the need for and extent of records. Records shall be kept of all business interruptions and incidents related to the BC.

Monitoring of Compliance

Monitoring is directed at ensuring the CEO of the compliance with main principles in Group and Local Policy Safeguarding of Assets and procedural action steps in accompanying procedures. BCM Program Manger is responsible for local monitoring activities. BCM program Manager shall annually perform an assessment of the compliance with policy and report the results of the assessment to CEO. BCM Program Manager will also ensure that Group self assessments survey for any area required from Group Risk.

BCM program Manager must report the number and type of exercises completed, the training conducted and the status of Securitysense-wide business continuity plans to CEO semi-annually.

Definitions

Business Continuity

The ability of Securitysense to ensure continuity and availability of service and support for customers, partners and the general public interest before, during and after a Crisis

Crisis

A Crisis is a situation that has a potentially dramatic impact on people, environment, assets, reputation or the ability to operate

Business Continuity / Crisis Exercise

An announced or unannounced execution of Business Continuity plans intended to implement or revise existing plans and/or highlight the need for additional plans to be developed

Business Continuity Management

Securitysense's overall response to a business continuity or crisis, with the purpose of avoiding or minimizing damage to its stakeholders, profitability, reputation or ability to operate

Business Continuity Program Manager

The Business Continuity/ Crisis Management Team Leader is the Manager of the Business Continuity Management Program.

Abbribiation

_

BCM	Business Continuity Management
BC	Business Continuity
CM	Crisis Managemen**t**

References:

- BS 25999-1:2006 Code of practice for business continuity management
- BS 25999-2:2007 Specification for business continuity management.