SECURITY SOLUTIONS

RISK MANAGED SECURITY ASSURED

Business Continuity Plan

Document Control

Filename: BS-01 - BCM Business Continuity Plan
Classification: In-Confidence
Author: Athar Awan
Owner: CISO

Version	Date Updated	Author	Description of Changes
1.0	10/09/2025	Athar Awan, CISO SSC	Initial Draft Document, build the possible scenarios
1.1	20/09/2025	Athar Awan, CISO SSC	Reviewed, Added/updated information

Purpose:

This Business Continuity Plan is intended to provide strategies to ensure that major issues relating to the GRCLens can be mitigated, to ensure minimal disruption to services. This plan should be considered supplementary to the Securityurity Solutions Business Continuity Plan.

Key Staff and Contacts:

Group	Team members (and contact details)
Data & Technical Capability	Athar Awan - CISO, Data and Technical capability Phone: +64204593800, +61451021750 Email: Athar.Awan@Securitysolutionshub.com
	Ali Raza – Associate GRC Consultant Phone: +61411225020 Email: ali.raza@Securitysolutionshub.com

Section 1: Introduction:

A. How to use this plan:

In the event of a disaster which interferes with the Security Solutions ability to conduct business from one of its site offices, this plan is to be used by the responsible individuals to coordinate the business recovery of their respective areas and/or offices. The plan is designated to contain, or provide reference to, all of the information that might be needed at the time of a business recovery.

Index of Acronyms:
(EOC) Emergency Operations Centre
(EMT) Emergency Management Team
(ERT) Emergency Response team
(BCP) Business Continuity Plan
(IT) Information Technology

Securitytion1, Introduction, contains general statements about the organisation of the plan. It also establishes responsibilities for the testing (exercising), training, and maintenance activities that are necessary to guarantee the ongoing viability of the plan.

Security 2, Business Continuity Strategy, describes the strategy that Security Solutions will control/implement to maintain business continuity in the event of a facility disruption. These decisions determine the content of the action plans, and if they change at any time, the plans should be changed accordingly.
Securitytion3, Recovery Teams,

Loss of IT Infrastructure/Key applications

Scenario 1a: Web Application Down, Security Solutions Operational	
Strategy	Escalate to Security Solutions
Minimum Requirements	Access to Security Solutions Service Desk, or email (either via Outlook) or Outlook Contacts

Is anything else required	Appropriate comms required to keep Security Solutions internally and customers informed
What are your options to mitigate risk?	Test changes/releases in the integrated Test Environment prior to Production
Recovery Point Objective	48 Hours. We could accept up to 48 hours of data being lost. It is likely that the real recovery point in this scenario would be close to a few hours as Security Solutions use cross region replication to ensure that multiple versions of GRCLens exist in multiple regions.
Recovery Time Objective	48 Hours as specified within Master Service Agreement
Maximum Tolerable Period of Disruption	3 working days

Time	Task	By whom	What and how is the task carried out
15 Mints	Establish extent of Issue	Security Solutions CISO	Check and verify how many customers are impacted
	Alert customer account manager of the issue	Security Solutions CISO/Associate	Email
	Raise Ticket via Service Desk tool or email	Security Solutions	Email
30 Mints	Contact key staff to advise that they are aware of the issue, and when the next update can be expected.	Security Solutions Associate GRC Consultant	Email
1 Hour	Liaise with staff to consider impact and potential workarounds	Security Solutions Associate GRC Consultant	Email, Mobile text or online chat
	If feasible, extract information from the Reporting Database to	Security Solutions Associate GRC Consultant	Azure SQL DB

	enable any immediate activities to continue		
	Follow up with customer account managers if confirmation has been received and to ensure that team is working for resolution	Security Solutions Associate GRC Consultant	Email/Phone call/text
4 Hours	Provide update to staff regarding current situation and expected return to BAU (if known)	Security Solutions Associate GRC Consultant	Email/text
	If return to BAU does not appear to be imminent, send updates to all impacted customers	Security Solutions Associate GRC Consultant/CISO	Email/text
Day 1-5	Maintain communications with internal staff and customers providing information from reporting DB to support ongoing activities	Security Solutions Associate GRC Consultant/CISO	Email/text

Scenario 1b: Web Application Up, customer's Integrated Services unavailable	
Strategy	Escalate to Security Solutions
Minimum Requirements	Access to Security Solutions Service Desk, or email (either via Outlook) or Outlook Contacts
Is anything else required	Contact information of Customer Relationship manager (TBD in future)
What are your options to mitigate risk?	Depend on customer plan
Recovery Point Objective	N/A

Recovery Time Objective	N/A
Maximum Tolerable Period of Disruption	N/A

Scenario 2: Loss of Primary Work Location	
Strategy	This scenario considers how to mitigate the effects of losing Primary work areas due to any natural disaster and on the ability of staff to continue supporting customers. The Strategy for this scenario is for staff to simply use their devices from home. As GRCLens is a SAAS web application so no reliance on staff using it from a specific location. Due to this, no timeline is required for resolution.
Minimum Requirements	Access to Security Solutions Service Desk, or email (either via Outlook) or Outlook Contacts and SAAS web application
Is anything else required	Contact information of Customer Relationship manager (TBD in future)
What are your options to mitigate risk?	As GRCLens is a SAAS web application so no reliance on staff using it from a specific location. Due to this, no timeline is required for resolution.
Recovery Point Objective	N/A
Recovery Time Objective	N/A
Maximum Tolerable Period of Disruption	N/A

Scenario 3: Loss of Key staff	
Strategy	Configuring and supporting Security Solutions Products required specialized skills, which is currently shared between a team of 4-5 people. This scenario considers the possibility of key persons being unavailable due to illness or vacations.
Minimum Requirements	Access to Security Solutions Service Desk, or email (either via Outlook) or Outlook Contacts and SAAS web application
Is anything else required	Contact information of Customer Relationship manager (TBD in future)
What are your options to mitigate risk?	Foster in house and cross domain training to enable the maximum team to support the product and services. Manage annual leaves well, ensuring key staff always have their devices available, in order to work from home when required. Ensuring that key Administration Processes are documented.
Recovery Point Objective	N/A
Recovery Time Objective	N/A
Maximum Tolerable Period of Disruption	N/A