

NIST 2.0 Incident Response Planner

Version: 0.1



Contents

Introduction.....	3
Cyber Incident Response Plan Creation.....	4
Cyber Incident Response Plan generation.....	8
Disaster declaration	8



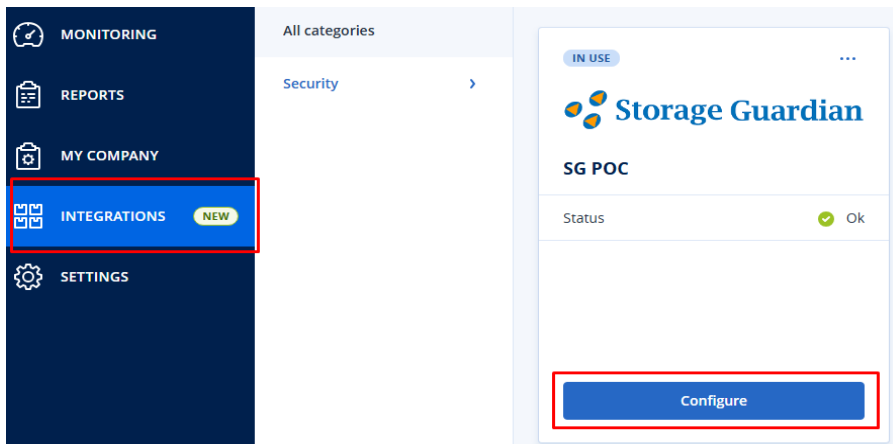
Introduction

An Incident Response Planner is a structured framework designed to help organizations effectively detect, respond to, and recover from security incidents, minimizing damage and downtime. It outlines predefined roles, responsibilities, communication protocols, and technical procedures to ensure a swift and coordinated response. A well-developed incident response plan enhances an organization's resilience by integrating proactive threat detection, containment strategies, forensic analysis, and continuous improvement measures. By leveraging industry best practices and compliance requirements, an Incident Response Planner helps mitigate risks, safeguard critical assets, and maintain business continuity in the face of cyber threats or operational disruptions.

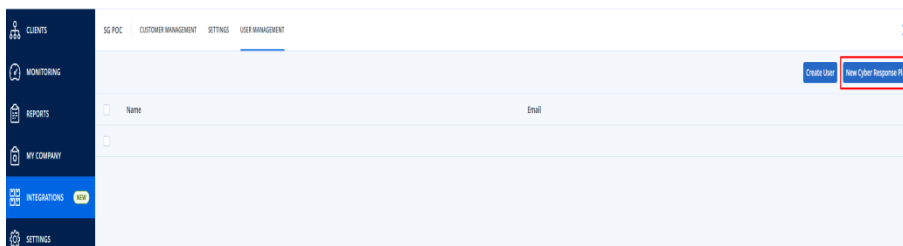


Cyber Incident Response Plan Creation

Search for “Storage Guardian” tile in the “Integrations” section of “Acronis Cyber Protect Cloud” platform and Click “Configure” button:



Choose a user and click “New Cyber Response Plan” from the “User Management” tab of the wizard:



Fill in the details: Plan Name, Organization Name, Months. The system will assign a PIN code automatically, but you can assign one you prefer as long as it is not taken. The last part is to add the CyberSecurity Incident Response team. Choose the roles from the drop-down menu. Click the Next button to continue:

New Cyber Incident Plan

Plan Name
plan_name

Organization
organization_name

Months
1

60203572

Add the following details of the Cybersecurity Incident Response Team:

Role	Name	Title	Phone	Email
Inciden...	John Johnson	CTO	+12345678	john@stora...
Inciden...	Martin Fern...	Tech Lead	+122345678	martin@sto...
Role	Name	Title	Phone	Email
Role	Name	Title	Phone	Email

Next



The External Contacts step appears (CyberSecurity Vendors, Incident Response Consultants, Cyber Insurance Providers, Internet Service Providers (ISPs), Affected Third Parties & Partners). Add any external contacts if you have any. If not, click the Next Button.

External Contacts

Contractor

Michael Cla...

Sr. Engineer

+123456

Michael@st...

Role

Name

Title

Phone

Email

Role

Name

Title

Phone

Email

Next

The other Stakeholders step appears (all individuals, teams, and external entities involved in or affected by CyberSecurity incidents). Add other Stakeholders if you have. If not, click the Next button.

Other Stake Holders

Stakeholder 1

Fred Johnson

Technical An...

+12345678

fred@sotra...

Role

Name

Title

Phone

Email

Role

Name

Title

Phone

Email

Next



The responsibilities stage appears. Add the responsibilities of each team. Click Next button to complete:

Responsibilities

Executive Responsibilities

Decision Maker

Responsibilities

Responsibilities

Incident Handler Responsibilities

Take Action According to Decisions

Responsibilities

Responsibilities

Communication Expert Responsibilities

Communicate Every Step

Responsibilities

Responsibilities

CSIRT Responsibilities

Respond To Cyber Incident

Responsibilities

Responsibilities

Staff Team Responsibilities

Responsibilities

Responsibilities

Responsibilities

Next



The PICERL (Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned) approach phase appears. Fill in the required fields specifically for your organization: for Preparation, Identification, Containment, Eradication, Recovery and Lessons Learned (This structured approach helps organizations respond to threats in a systematic, efficient, and effective manner, minimizing damage and strengthening CyberSecurity resilience). Click Next to complete:

A screenshot of a web form titled "PICERL" with a close button (X) in the top right corner. The form is labeled "INCIDENT HANDLING PROCESS" and contains six text input fields, each with a placeholder label: "Preparation", "Identification", "Containment", "Eradication", "Recovery", and "Lessons Learned". At the bottom left of the form is a blue button labeled "Next".

The ISHP stage appears. ISHP stands for Initial Security Handling Procedures (it refers to the standardized processes and guidelines that organizations follow when responding to a CyberSecurity incident in its early stages). Fill in the required fields and click Finish:

A screenshot of a web form titled "ISHP" with a close button (X) in the top right corner. The form is divided into five sections, each with a header and three text input fields: "Data Breach", "Ransomware", "Tampering of Payment Terminals", "Widespread Service Interruption", and "Loss of Equipment". At the bottom left of the form is a blue button labeled "Finish".

Cyber Incident Response Plan generation

Disaster declaration

There are three ways to declare a disaster:

1. Declaration via the IVR system

- Dial +1.226.210.1614
- Click 1 for declaring a disaster
- When prompted, the IVR system will request you to enter your PIN number
 - If the PIN number is correct, IVR will notify Storage Guardian about the request for DRaaS
 - If the PIN code is incorrect, the IVR system will prompt you to enter the 8-digit PIN again
 - After three failed attempts, the IVR system will hang up, and a representative from Storage Guardian will contact you on your phone number to review your DRaaS request



Dial



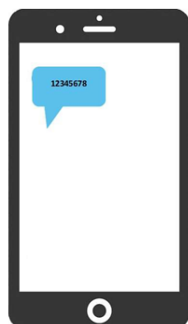
via the IVR system
Press 1 to declare a cyber incident.
Press 2 to declare DR.
Press 3 to declare a Cyber Test.
Press 4 to declare a DR Test.



Enter the Pin Number to
Declare Cyber Incident

2. Declaration via Text messaging

- Send the pin code number to +1.226.210.1614
- You will get a text back saying the fast failover for the disaster recovery process has started.



Text the
Pin code



Disaster declaration
confirmation

3. Declaration via Web

- Navigate to: <https://drsetup.azurewebsites.net/Home/PIN>
- Enter the customer Username and Password



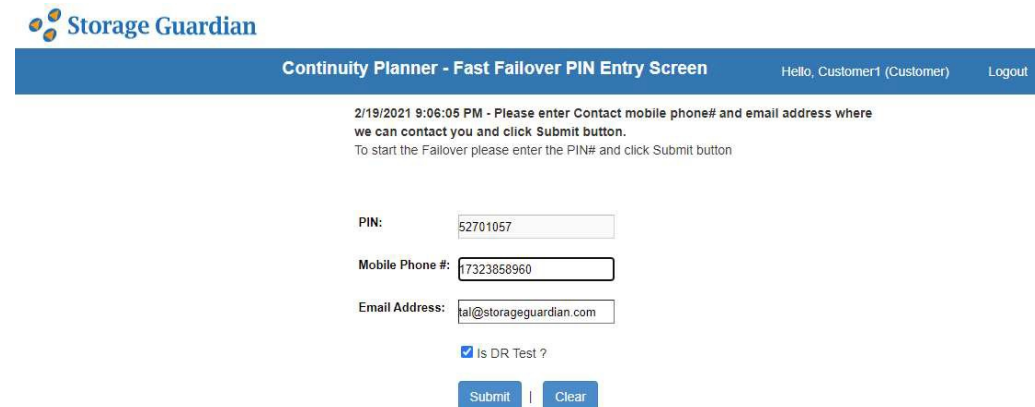
The screenshot shows the 'Storage Guardian' logo at the top left. Below it is a blue header bar with the text 'DR Runbook - Declaration'. The main content area is titled 'DR Runbook Declaration- Login'. It contains a login form with two input fields: the first is labeled 'AcmeDemo' and the second is a password field with masked characters and an eye icon. Below the password field is a blue 'Log-in' button. At the bottom of the form is a link that says 'Forgot password?'.

- After logging in, the following window appears:



The screenshot shows the 'Storage Guardian' logo at the top left. Below it is a blue header bar with the text 'DR Runbook - PIN Entry Screen'. On the right side of the header bar, it says 'Hello, acmedemo (MSP)' and 'Logout'. The main content area has a message: 'To start the Declaration please enter the PIN# and click Submit button'. Below this is a form with a 'PIN:' label and an input field. Under the input field is a checkbox labeled 'I'm not a robot' and a reCAPTCHA logo. Below the checkbox is a link that says 'Is Test?'. At the bottom of the form are two buttons: 'Submit' and 'Clear'.

- Verify that you are not a robot by checking the check box and going through the verification process. Once verified, enter your pin number
- Check the "is DR Test" check box. (DR Test indicates that the Disaster Declaration is for Testing purposes and is not taken to be an actual one)
- Click the Submit button



The screenshot shows the 'Storage Guardian' logo at the top left. Below it is a blue header bar with the text 'Continuity Planner - Fast Failover PIN Entry Screen'. On the right side of the header bar, it says 'Hello, Customer1 (Customer)' and 'Logout'. The main content area has a message: '2/19/2021 9:06:05 PM - Please enter Contact mobile phone# and email address where we can contact you and click Submit button. To start the Failover please enter the PIN# and click Submit button'. Below this is a form with three input fields: 'PIN:' with the value '52701057', 'Mobile Phone #:' with the value '17323858960', and 'Email Address:' with the value 'tal@storageguardian.com'. Below the input fields is a checkbox labeled 'Is DR Test ?' which is checked. At the bottom of the form are two buttons: 'Submit' and 'Clear'.

