RESOLUTE GUARD

Central San Joaquin Valley Risk Management Authority
CSJVRMA

User-Friendly Cyber Risk Management Platform For RMA Insureds

---

Smart Workflow Management Solution Aligns:

- **Client Initiatives with Insurance and Regulatory Objectives**
- **Executive Governance with Administrative and Technical Activities**

To Guard Against A Cyber Disruption Of Service

RESOLUTE GUARD

Central San Joaquin Valley Risk Management Authority
CSJVRMA

Client Alignment with Insurance Objectives

As Ransomware and Other Cyber-Attacks Increase Insurance Coverage Costs and Terms are also Increasing

Lowering of Coverage Limits
Increasing Premiums and Deductibles
Limited or No Ransomware coverage

Insurance Providers Are Requiring Detailed Questionnaires to Determine Insurance Renewal Costs and Terms

RESOLUTE GUARD

Central San Joaquin Valley Risk Management Authority
CSJVRMA

Cyber Insurance Coverage
Public Entity Minimum System Security Standards

Patching- Updated within 30 days; 1-7 days for Critical & High Severity patching

Guidelines/Policies- Incident Response; Disaster Recovery; Business Continuity

Backups- Separate from Primary Network; Regular Backups; Testing; Encryption; Restore within 72 Hours, Anti-Virus

Multi-factor Authentication (MFA)- 100% for Remote Access and Privileged User Accounts; Email Access

Endpoint Protection, Detection & Response (EDR)- EDR Solution in place across Enterprise

Remote Desktop Protocol- MFA Enabled VPN Remote access; Network-level Authentication enabled

Employee Training- Simulated Phishing Email Training; Regular Cyber Security Training; Fraudulent Accounting Transactions

End of Life Software- Plan/Guidelines and Adequate Measures to Protect EOL Software

RESOLUTE GUARD

Central San Joaquin Valley Risk Management Authority
CSJVRMA

Cyber Security is Not Exclusively an IT Problem

Conduct Scans to Identify Current Networks Internal & External "Strengths and Weaknesses"

Prioritize Implementing the Solutions to the "Most at Risk" Vulnerabilities

Document the Guidelines and the Maintenance Activities that Fortify Solutions in Place

Conduct Scans Every 90 Days to Measure Progress and Change

Align Client Initiatives with Insurance and Regulatory Objectives
And Governance Oversight with Technical and Administrative Activities

SMART-CAP's Align Insured Workflow With Insurance Objectives

RESOLUTE GUARD

Smart Cyber Action Plan ™ (S-CAP)
Insured 1 - 50 Devices

*Insurance Renewal - 7/1/22
*Insurance Question
* Scan Date - 3/30/22

Account Manager
accountmanager@resoluteguard.com

Score		Security Profile Model						Guidelines	
Pers	Act		Solution	Status	Next Steps	Date	Assigned	Guideline	Status
		Backup/Firewall/Incident Response/Service Continuity							
6	6	*Have you designated a Cyber Security/Privacy Officer w/ a Cyber Action Plan?	Policy	Pre-Scan			Conner S	D.AM-6, ID.GV-	Complete
4	0	Is your backup encrypted, segmented with seperate login credentials	Unitrends	Pre-Scan		8/3/2022	John D	R.AC-5, PR.IP-	In Progress
4	4	*Do you perform and regularly test data backups?	Unitrends	Pre-Scan				PR.IP-4	Complete
4	0	Are Firewalls in place, up-to-date, and configured?	Fortinet	Pre-Scan		8/3/2022	Mike L	PR.IP-1-2	In Progress
4	4	*Do you have a written Incident Response Policy?	Policy	Pre-Scan				PR.IP-9-10	Complete
4	0	*Do you have a Business Continuity Policy?		Pre-Scan				PR.IP-9-10	In Progress
		User Protection							
4	2	*Do you provide user awareness training?	Bullphish	Pre-Scan				PR.AT-1-5	Not Started
4	0	*Do you have MFA enabled for all employees?	Passly	Pre-Scan				PR.AC-1	Not Started
4	4	*Do you conduct simulated email phishing testing?	Bullphish	Pre-Scan				PR.AT-1-5	Not Started
4	0	Are strong passwords checked every 90 days and set to expire?	CAP	Pre-Scan				PR.AC-1	Not Started
4	4	*Does your email software scan for malicious links or attachments?	Graphus	Pre-Scan				PR.DS-2	Complete
4	4	*Does your email protection software block and/or notate suspicious emails?		Pre-Scan		6/1/2022	Jane D	PR.DS-2	Complete
		Data Protection							
4	0	Do you have Business Associate Agreements with 3rd party vendors?	Policy	Pre-Scan				PR.AC-4	Not Started
4	0	Are inactive users purged from the Active Directory?		Pre-Scan				PR.IP-11	Not Started
4	0	Are you incorporating principles of least priviledge and separation of duties		Pre-Scan				PR.IP-11	Not Started
4	0	*Do you comply with relevant PII requirements?		Pre-Scan		1/1/2023	Bob H	AM-6, ID.GV-2,	Not Started
4	0	Are you HIPAA compliant?	CAP	Pre-Scan		1/1/2023	Bob H	AM-6, IM.GV-2,	Not Started
4	0	Are you PCI compliant?		Pre-Scan		1/1/2023	Bob H	AM-6, IM.GV-2,	Not Started
		Network							
6	3	*Do you conduct internal/external vulnerability scans?	Vulscan	Pre-Scan				ID.GV-1	Not Started
4	0	Do you have network threat monitoring software?	Cyber Hawk	Pre-Scan				ID.GV-1	Not Started
4	2	*Do you have Anti-virus and Anti-Malware installed on all devices? Reuglarly Scanning?	Bitdefender	Pre-Scan		9/1/2022	Steve K	ID.AM-2	Not Started
4	0	*Do you have an Endpoint Intrusion Detection and Response solution?	Rocket Cyber	Pre-Scan				ID.AM-2	Not Started
4	0	Do you update/patch hardware and software regularly?	Excel Worksheet	Pre-Scan		9/1/2022	Steve K	ID.AM-1-2,	Not Started
4	0	Do you monitor for inactive computers? Rogue Computers?		Pre-Scan				PR.MA-1	Not Started
100	33								

SPM | Maintenance | Smart CAP | Policies

RESOLUTE GUARD

Document “Best Practices” Guidelines To Support Continuous Improvement

Guidelines and Procedures
Mapped to NIST Standards

Data Backup Guideline
Incident Response Plan
Business Continuity Plan
Password Management
Acceptable Use
Email Guideline
Access Control
Awareness Training
and more…

Introduction

Data Backup Guideline

The [Company] Data Backup Plan has been developed to provide guidance to the protection of information whose loss would adversely affect [Company] **Information Resources**. The [Company] Data Backup Plan applies to any person or entity charged by the [Company] with safeguarding data assets.

The purpose of the Data Backup Plan is to allow [Company] minimize vulnerability and to respond quickly and appropriately to restore availability of data during a data loss incident. The Security Officer must develop a comprehensive plan to back up organization data and critical applications or implements fault-tolerant systems that reduce the likelihood that equipment failure or disasters will adversely affect the integrity and availability of organization data.

Backup Definition

This document provides recommendations to help *[Company]* conduct, maintain, and test backup files ***to*** reduce the impact of data loss incidents. A backup file is a copy of files and programs made to facilitate recovery. Technical workforce members responsible for preparing back-up data sets must test the back-up copies at least every 3 months to ensure that they:

- Contain an exact copy of the information they back up
- Can be restored when needed

Adverse Events Definition

Data loss incidents—whether a ransomware attack, hardware failure, or accidental or intentional data destruction—can have catastrophic effects *on [Company]* and their customers.

Incident Definition

Backup systems implemented and not tested or planned increase operational risk for Organizations. The impacts of data loss events can include one or more of the following:

A. loss of productivity
B. revenue/customer loss
C. negative reputation and brand impacts
D. Loss of [Company] Confidential or Protected information

Reference

- NIST SP800-53, Rev 4 CP-9 Contingency Planning Information Systems Backup:

RESOLUTE GUARD

Table of Contents

RESOLUTE GUARD

Data Backup Framework

[Company] recognizes that, despite reasonable and competent efforts to protect **Information Resources**, a breach or other loss of information is possible. The organization must make reasonable efforts and act competently to respond to a potential incident in a way that reduces the loss of information and potential harm to customers, partners, and the organization itself.

Developing a well-defined Data Backup framework is critical to an effective Data Backup plan. The [Company] Data Backup framework is comprised of six phases that ensure a consistent, flexible, and systematic approach.

Phase I – Preparation
It is essential to establish a Cyber Security Data Backup Team (CSDBT), define appropriate lines of communication, articulate services necessary to support response activities, and procure the necessary tools. Backup plans are documented to comply with all applicable requirements

Phase II – Identification and Assessment
Identify the files to back up. Prioritize files based on business value. For example, an organization may not be able to backup all files due to cost, size, or accessibility. Examples of key files are event logs, user files, and applications. Prevent data from being stored in locations that are not backed up. See NIST SP 800-53, Rev. 4, AU-9, Protection of Audit information, for more information.

Phase III – Restoration time
Establish the desired timeframe to restore files and applications to minimize negative impacts to the organization’s mission or business operations–known as recovery time objective (RTO).

Phase IV – File Backup Timing
Determine maximum age of the backup files to enable operations to be reestablished with minimum acceptable interruption of operations–known as the recovery point objective (RPO). Acceptable backup file age may vary based on the file types and business process impacted (operations, human resources, accounting, for example).

RESOLUTE GUARD

Manage the Maintenance Activities that Fortify Solutions in Place

Guidelines				
Guidelines	**NIST - CSF**	**Status**	**Date**	**Assigned**
Backup and Retention Plan Template	PR.IP-4	Complete	2/1/2022	Robert S
Incident Response Plan	PR.IP-9, 10	Complete	1/1/2022	Joe D
Business Continuity Plan Policy Template	PR.IP-9, 10	Complete	3/1/2022	Matt L
Baseline Configurations - System Development Life Cycle Policy Template	PR.IP-1-2	Complete	3/2/2021	CJ M
Password Management Authentication Policy Template	PR.AC-1	Not Started		
Network Segregation_Segmentation Policy Template	PR.AC-5	Not Started		
Access Control Policy Template	PR.AC-1	Review	4/21/2022	Zach W
Assigned Security Responsibility Policy Template	ID.AM-6	In Progress	5/5/2022	Elijah M
Automatic Log-Off Policy Template	PR.DS-5	Complete	4/1/2022	Corey D
Awareness and Training Policy Template	PR.AT-1-5	Research	4/12/2022	Braxton B
Change Control Policy Template	PR.IP-3	Not Started		
Client Access Passwords Policy Template	PR.AC-1	Not Started		
Client Security Policy Template	ID.AM-6, ID.GV-2	Not Started		
Compliance Policy Template	ID.AM-6, ID.GV-2, 3, 4	Not Started		
Data Backup Policy Template	PR.IP-4	Not Started		
Data Leakage Policy Template	PR.DS-5	Not Started		
Data-At-Rest Policy Template	PR.DS-1, PR.PT-2	Not Started		
Developement-Testing Policy Template	PR.DS-7	Not Started		
Disposal of Assets and Data Policy Template	PR.IP-6	Not Started		
Documentation Policy Template	ID.AM-1, 2	Not Started		
E-Mail Policy Template	PR.DS-2	Not Started		
Hardware Inventory Policy Template	ID.AM-1	Not Started		
Human Resources Alignment Policy Template	PR.IP-11	Not Started		
Information Access Managment Policy Template	ID.AM-6	Not Started		

SPM | Maintenance | Smart CAP | **Policies**

RESOLUTE GUARD

Industry Best Internal / External Scanning Tools

Identify Strengths and Weaknesses in Alignment with Regulatory Objectives

in Accordance with the United States

National Institute of Standards & Technology Cyber Security Framework (NIST-CSF)

Universal “Gold Standard” Framework

Mandated / Recommended as a Basis For All Government Programs

Continuously Updated With Newly Identified Cyber Risk

RESOLUTE GUARD

Industry Best Scanning Tools Provide a Documented Inventory of Your Cyber Risk Strengths and Weaknesses

Computer Name	Operating System	Install Date	Age (Months)	Physical or VM	Status
Server 1	Windows Server 2003	5/31/2007 15:56	175	Virtual Machine	Vulnerable - payroll system on older server version
Server 2	Windows Server (R) 2008 Enterprise	4/7/2009 12:56	152	Physical	
Server 3	Windows Server 2008 R2 Enterprise	8/18/2010 13:56	136	Physical	Feb 15th goes offline
Server 4	Windows Server (R) 2008 Enterprise	10/26/2010 14:52	134	Physical	
Server 5	Windows Server (R) 2008 Standard	8/17/2011 18:49	124	n/a	
Server 6	Windows Server (R) 2008 Standard	8/18/2011 23:52	124	n/a	

Computer Name	Operating System	Install Date	Age (Months)	Physical or VM	Status
FrontDesk-1	Windows 7 Professional	4/16/2010 1:24	140	Physical	Admin buidling Windows 7/older hardware currently being replaced.
JaneDoe	Windows 7 Professional	4/20/2010 12:57	140	Physical	Chip shortage affecting hardware refresh program
Library	Windows 7 Professional	7/1/2010 8:52	137	Physical	
ComputerLab-1	Windows 7 Professional	7/21/2010 11:32	137	Physical	Test
Mathlab2	Windows 7 Professional	8/5/2010 13:18	136	Physical	Replacing February 22nd
Superintendent-1	Windows 7 Professional	10/4/2010 16:07	134	Physical	
JohnDoe	Windows 7 Professional	10/27/2010 8:21	134	Physical	

Environment | Smart CAP | SPM | Policies | External | Maintenance | Completed Actions | Schedule

RESOLUTE GUARD

Easy To Understand Smart Workflow Reports Align Governance Oversight with Administrative / Technical Activities

Immediate Action List

High Risk

Risk Score	Recommendation	Severity	Probability
97	Upgrade or replace computers with operating systems that are no longer supported. ☐ HTPC / ::1,10.0.0.201 / Windows 7 Professional	H	H
94	To prevent both security and productivity issues, we strongly recommend ensuring that anti-virus is deployed to all possible endpoints. ☐ Computer: WINMANAGESERVER IP Address: 10.0.0.1	H	H
94	Assure that anti-spyware is deployed to all possible endpoints in order to prevent both security and productivity issues. ☐ Computer: WINMANAGESERVER IP Address: 10.0.0.1	H	H
90	Address patching on computers missing 4+ security patches. ☐ HTPC / ::1,10.0.0.201 / Windows 7 Professional	H	H
85	Evaluate the risk, cost, and benefits of implementing a redundant Domain Controller.	H	H

SMART-CAP's Align Insured Workflow With Insurance Objectives

RESOLUTE GUARD

Smart Cyber Action Plan ™ (S-CAP)

Insured 1 - 50 Devices - Scan Scheduled - 5/30/22

*Insurance Renewal - 7/1/22
*Scan Scheduled 5/30/22

Score		Smart-CAP Pre-Scan (SPM) Scoring			Guidelines	
Poss	Act		Solution	Status	Guidelines	Status
		Backup/Firewall/Incident Response/Service Continuity				
6	6	*Have you designated a Cyber Security/Privacy Officer w/ a Cyber Action Plan?	Policy	Complete	ID.AM-6, ID.GV-2	Complete
4	2	*Is your backup encrypted, segmented with separate login credentials	Unitrends	Complete	PR.AC-5, PR.IP-4	In Progress
4	4	*Do you perform and regularly test data backups?	Unitrends	Complete	PR.IP-4	Complete
4	0	*Are Firewalls in place, up-to-date, and configured?	Fortinet	Not Started	PR.IP-1-2	In Progress
4	4	*Do you have a written Incident Response Policy?	Policy	Complete	PR.IP-9-10	In Progress
4	0	*Do you have a Business Continuity Policy?		Not Started	PR.IP-9-10	In Progress
		User Protection				
4	0	*Do you provide user awareness training?	Bullphish	Sourcing	PR.AT-1-5	Not Started
4	0	*Do you have MFA enabled for all critical applications?	Passly	Sourcing	PR.AC-1	Not Started
4	0	Do you conduct simulated email phishing testing?	Bullphish	Budgeting	PR.AT-1-5	Not Started
4	2	Are strong passwords checked every 90 days and set to expire?	CAP	Complete	PR.AC-1	Not Started
4	2	Does your email software scan for malicious links or attachments?	Graphus	Complete	PR.DS-2	Not Started
4	0	Does your email protection software block and/or notate suspicious emails?		In Progress	PR.DS-2	Not Started
		Data Protection				
4	2	*Is Confidentiality, Integrity, and Availability of information securely managed?	Policy	Complete	PR.AC-4	Not Started
4	0	Are inactive users purged from the Active Directory?		Not Started	PR.IP-11	Not Started
4	0	Are you incorporating principles of least priviledge and separation of duties		Not Started	PR.IP-11	Not Started
4	0	Do you comply with relevant PII requirements?		In Progress	D.AM-6, ID.GV-2,3,	Not Started
4	0	Are you HIPAA compliant?	CAP	In Progress	D.AM-6, IM.GV-2,3	Not Started
4	0	Are you PCI compliant?		In Progress	D.AM-6, IM.GV-2,3	Not Started
		Network				
6	4	*Do you conduct internal/external vulnerability scans?	Vulscan	Complete	ID.GV-1	Not Started
4	0	*Do you have network threat monitoring software?	Cyber Hawk	Not Started	ID.GV-1	Not Started
4	0	*Do you have Anti-virus and Anti-Malware installed on all devices?	Bitdefender	Budgeting	ID.AM-2	Not Started
4	0	*Do you have an Endpoint Intrusion Detection and Response solution?	Rocket Cyber	Complete	ID.AM-2	Not Started
4	0	*Do you update/patch hardware and software regularly?	Excel	In Progress	ID.AM-1-2,	Not Started
4	0	Do you monitor for inactive computers? Rogue Computers?	Worksheet	Not Started	PR.MA-1	Not Started
100	26					

Environment | **Smart CAP** | SPM | Policies | External | Maintenance | Completed Actions | Schedule

RESOLUTE GUARD

Manage the Maintenance Activities that Fortify Solutions in Place

Maintenance Schedule

Maintenance - Q1

Requirement	Cadence	1/1/2022	1/8/2022	1/15/2022	1/22/2022	1/29/2022	2/5/2022	2/12/2022	2/19/2022	2/26/2022	3/5/2022	3/12/2022	3/19/2022	3/26/2022
Password Reset	30 days	Complete				Complete				Complete				
Patching	7 days	Complete	Complete	Complete	Complete	Complete	Complete	Complete	Complete	Complete	Complete	Complete		
Backup	7 days	Complete	Complete	Complete	Complete	Complete	Complete	Complete	Complete	Complete	Complete	Complete		
AD Cleanup	Quarterly	Complete												
Training	Quarterly	Complete												
Policy Refresh	Semi-Annually	Complete												
Hardware Refresh	Yearly	Complete												
Software Refresh	Yearly	Complete												
Network Segregation	Yearly	Complete												

Maintenance - Q2

Requirement	Cadence	4/2/2022	4/9/2022	4/16/2022	4/23/2022	4/30/2022	5/7/2022	5/14/2022	5/21/2022	5/28/2022	6/4/2022	6/11/2022	6/18/2022	6/25/2022
Password Reset	30 days													
Patching	7 days													
Backup	7 days													
AD Cleanup	Quarterly													
Training	Quarterly													
Policy Refresh	Semi-Annually													
Hardware Refresh	Yearly													
Software Refresh	Yearly													
Network Segregation	Yearly													

Maintenance - Q3

Requirement	Cadence	7/2/2022	7/9/2022	7/16/2022	7/23/2022	7/30/2022	8/6/2022	8/13/2022	8/20/2022	8/27/2022	9/3/2022	9/10/2022	9/17/2022	9/24/2022
Password Reset	30 days													
Patching	7 days													
Backup	7 days													
AD Cleanup	Quarterly													
Training	Quarterly													

RESOLUTE GUARD

Central San Joaquin Valley Risk Management Authority
CSJVRMA

Progress & Change is Reviewed Every 90 Days

Internal / External Scan Updates Your "**Strengths and Weaknesses**"

Incorporates Progress Made and Any Newly Identified NIST-CSF Risks

Updates & Re-Prioritizes Cyber Action Plan (SMART-CAP) Activities by Risk of Loss

Smart Workflow Management Supports Continuous Improvement

RESOLUTE GUARD

Central San Joaquin Valley Risk Management Authority
CSJVRMA

“Easy to Use” Data Collector

“Easy to use” data collector software is locally installed and requires no hardware.

Safe and non-disruptive, causes no conflict with other applications or firewalls, and requires zero maintenance.

A 30-minute remote call is set with your assigned resource to activate the tool and collect all your hardware, software and network “strengths and weaknesses” data.

This provides a comprehensive documented view of your current environment.

Knowing “where you are” empowers you to identify the best steps to “Do the Best You Can as Fast As You Can”

RESOLUTE GUARD

Central San Joaquin Valley Risk Management Authority
CSJVRMA

“Easy to Understand” Data Collector Process

1- INTERNALLY scan to identify status of:

- Azure and Microsoft Office 365 Cloud Services
- Local servers and computers versions
- Software applications and user-access

2- Individually scans:

- LINUX and MAC OS (non-Windows) devices on your network.
- SQL Databases for unencrypted Personal Identifiable Information (PII)
- EXTERNAL ports for open, unsecure, outdated services and listening agents

3- Provides “current status” reports and diagrams, prioritized by risk, to create Cyber Action Plan:

- Back-up, firewall, incident response, and business continuity plans
- OS, inactive computers, application and endpoint Patches, endpoint Security
- Inactive Users, user access permissions and shares, PII management

RESOLUTE GUARD

Cyber Risk Management Platform
Smart Workflow Benefits

User-friendly Platform Aligns Administrative and Technical Cyber Security Activities

- **Easy Onboarding and Engagement**

Customized To Your Specific Insurance Questionnaires and Requirements

- **To Take the Best Actions to Align Cyber Insurance**

Leverages Industry Best Tools to Identify Internal / External “Strengths and Weaknesses”

- **Manage Cyber Risk as New technology is Introduced / Obsolete Systems are Updated or Replaced**

Prioritizes Activities by Risk of Loss Into “Easy to Use” Cyber Action Plans (SMART-CAP)

- **Empowers Governance to ensure sufficient resources are allocated to properly mitigate risk profile**

Automates “Easy to Understand” Reports and “Best Practices” Policies

- **Smart Workflow eliminates wasted resource efforts, improves efficiency of security practices**

Progress & Change is Reviewed Every 90 Days to Update and Re-Prioritize the Cyber Action Plan (SMART-CAP)

- **Updates Your “Strengths and Weaknesses;” Progress Made; and Any Newly Identified NIST-CSF Risks**

RESOLUTE GUARD

Central San Joaquin Valley Risk Management Authority
CSJVRMA

Next Steps

1. Review Services Agreement to Get Started
2. Once Signed, ResoluteGuard Schedules OnBoarding call
3. Review SMART-CAP (Pre-Scan)
4. Conduct Vulnerability Scan & Schedule Report Review
5. ResoluteGuard Updates SMART-CAP and Conducts Review

Questions?

Contact: support@resoluteguard.com

888-728-6030