Information Systems and Technology Security

Business Resilience and BCP Policy

Original author's name:	Pkkirisankar Jagannath
Most recent date:	March 22, 2023
Most recent version number:	v1.0
Process owner:	Program Director

Document History

Version	Date	Revised by	Description
v1.0	March 8, 2023	Pkkirisankar Jagannath	Original Draft
v1.0	March 22, 2023	Kulpreet Singh	Ratified Version

Designated document recertification cycle in days:	[Cycle 30 90 180 **365**]
Next document recertification date:	March 22, 2024

Acceptable Use Standard

As stated in the **22nd Century Technologies** (the "Company") **Business Resilience and BCP Policy**, the Company will follow a risk management approach to develop and implement information security policies, standards, guidelines, and procedures. The Information Security Program will protect information assets by establishing policies to identify, classify, define protection and management objectives, and define acceptable use of Company information assets.

This Acceptable Use Standard defines Company objectives for establishing specific standards on appropriate business use of the Company's information and telecommunications systems and equipment.

1. Scope

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company premises, or who have been granted access to Company information or systems, are covered by this policy and must comply with associated standards and guidelines.

The Company **Business Resilience and BCP Policy** and relevant policies, standards and guidelines must have fundamental guidance, procedures, and commentary based upon the ISO 27001 framework.

The ISO 27001 standard is a code of practice for information security subject to the guidance provided within ISO 27001.

The actual controls listed in the standard are intended to address the specific requirements identified via a formal risk assessment. The standard is also intended to provide a guide for the development of organizational security standards and effective security management practices.

2. Objectives

22nd Centuries Business Resiliency Plan is meant to work as per Business Resiliency and Business Continuity Plan, the goal is to create a plan that will help to respond to most emergency situations and recover as quickly as possible. If more space is needed on any of the tables provided in this worksheet, they are provided on a single page, so that you can print out more copies.

The BCP Team will Start by identifying the critical business functions and their supporting resources. Using the Business Resilience Guide, identify risks that the business could face, including ones that may not be listed in the guide. Analyze how these risks could affect the critical business functions and resources, including cashflow. With this information BCP team will create a business continuity plan (as well as the communications plan from the Business Resiliency Guide).
Then fill in the preventative measures which can be taken to mitigate risk from the most likely hazards, and perhaps unlikely sources. The final step is making the necessary contacts or preparations so that 22nd Century relevant Stakeholders ready to implement the plan when it is needed.

In the identify section of the Business Resource Guide identify the hazards the business is most exposed to and their severity. The last section of this business resiliency plan provides a template for BCP team to take those hazards and develop emergency response plans. These plans encompass both preparation for hazards and the appropriate actions to take in reaction.

3. Process

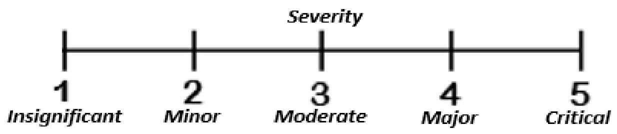
Business Goals

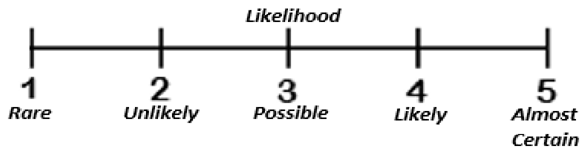
Goals	
1.	Recognize potential threats to a company.
2.	Assess potential impacts on the company's daily activities.
3.	Provide a way to reduce these potential problems and establish a structure that allows key company functions to continue throughout and after the event.
4.	Identify the resources the organization needs to continue operating, such as staffing, equipment, and alternative locations.

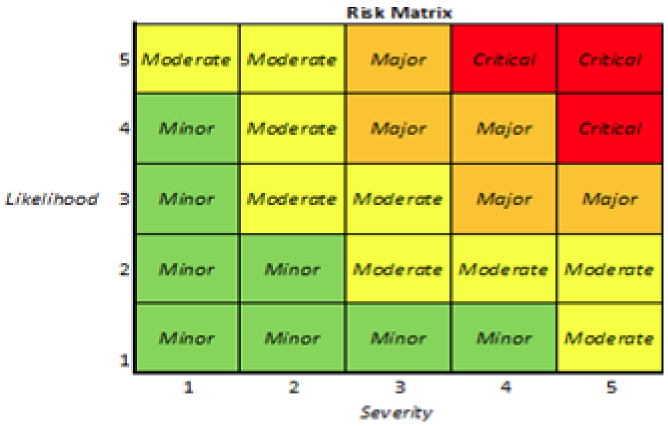
Critical Business Functions and Resources:

These are 22nd Centuries critical business functions and the resources they need. Without these our company cannot continue to operate.

Critical Business Function	Supporting Resource(s)	Function of Resource	Backup Resource(s)
Support		System Slowness Issue	Stock
	IT Helpdesk	New Software/Hardware Requirement	Stock
Data Management		Shared Drives	Backup Server
	IT Helpdesk	Shared Drives	SharePoint online
		Outlook PST	Cloud Storage
Infrastructure		Computers	Backup Server
	IT Helpdesk	Network devices	Backup Server
		Printers	Backup Server
Communication		Outlook	Office 365 exchange
	IT Helpdesk	Desk Phones	Cloud Portal
		Chat System	Office 365 exchange
Security		Firewall	Auto backup to Cloud Storage
	IT Helpdesk	Cybersecurity	Backup to Cloud Storage







Risk Matrix

Likelihood					
5	Moderate	Moderate	Major	Critical	Critical
4	Minor	Moderate	Major	Major	Critical
3	Minor	Moderate	Moderate	Major	Major
2	Minor	Minor	Moderate	Moderate	Moderate
1	Minor	Minor	Minor	Minor	Moderate
	1	2	3	4	5
	Severity				

Hazards

Our business is exposed to the following hazards. These could affect our critical business functions, preventing us from continuing business.

Human Caused HAZARD	How Likely? (1-5)	How Severe? (1-5)	Risk
Operational Risk	2	2	The risk of loss resulting from many normal aspects of business
Reputational Risk	1	1	A threat or danger to the good name or standing of a business or entity
Human risk	2	3	Loss to an organization caused by human factors including the decisions and non-decisions, actions, and non-actions of its people
Security risk	2	3	Security risk is the potential for losses due to an information security incident
Financial risk	3	3	Financial risk is the possibility of losing money on an investment or business venture
Physical risk	2	3	Risks which arise from the physical effects of climate change and environmental degradation

Natural HAZARD	How Likely? (1-5)	How Severe? (1-5)	Risk
Thunderstorm	3	2	Refer to power outage/blackout and medical emergency
Hurricane/Tropical Storm	3	2	Refer to power outage/blackout and medical emergency
Flooding	2	3	Office reachability impacted, power outage, risk of shock/electrocution
Winter Storm or Extreme Cold	3	3	Refer to "Power Outage/ Blackout" and "Medical Emergency,"
Extreme Heat	2	2	Refer to "Power Outage/ Blackout" and "Medical Emergency,"
Tornado	3	2	Refer to "Power Outage/ Blackout" and "Medical Emergency,"
Earthquake	2	3	Refer to "Power Outage/ Blackout" and "Medical Emergency,"
Pandemic Influenza	2	3	Refer to "Medical Emergency,"

Our backup Suppliers:

Supplier Name	Resources Supplied	Threats They Face	How Likely? (1-5)	How Severe? (1-5)	Risk
AWS/Microsoft	Cloud Storage	corrupted backup	2	2	Old media can get damaged or corrupted through poor handling or simply through age
		inaccessible backup	2	3	during a disaster, you can't use it to restore your data.
		slow backup	2	2	Slow backup procedures can cause delays that impact the start of work the next day

Backup Supplier 1: Company Name: AWS S3 Address: Cloud Portal		
Phone:	Fax:	E-mail: support@aws.com
Contact Name: Support		Account Number:
Materials/Service Provided: Cloud Storage		
Backup Supplier2 Company Name: Microsoft Address: Cloud		
Phone: (800) 642 7676	Fax:	E-mail: support@microsoft.com
Contact Name: Support		Account Number
Materials/Service Provided: Cloud Storage		

Our backup Distributors:

Distributor/ Client Name	Product Distributed	Threats They Face	How Likely? (1-5)	How Severe? (1-5)	Risk
AWS/Microsoft	Cloud Storage	corrupted backup	2	2	Old media can get damaged or corrupted through poor handling or simply through age
		inaccessible backup	2	3	during a disaster, you can't use it to restore your data.
		slow backup	2	2	Slow backup procedures can cause delays that impact the start of work the next day

Backup Distributor 1: Company Name: AWS Address: Cloud		
Phone:	Fax:	E-mail: support@aws.com
Contact Name:		Account Number
Materials/Service Provided: Cloud Storage		
Backup Distributor 2: Company Name: Microsoft Address: Cloud		
Phone: (800) 642 7676	Fax:	E-mail: support@microsoft.com
Contact Name:		Account Number
Materials/Service Provided: Cloud Storage		

Business Impact Analysis

If one of the above threats takes place these will be the likely business functions and resources affected. If one of these resources or functions is lost, we should work quickly to replace it.

Disaster	Resources Impacted	Recovery Time Objective	Operational Impacts	Financial Impacts
Power outages	Data Center Down	1 hour	Domain Services	No impact
	All Systems Down	1 hour	System access	No impact
Network outages	Firewall	30 mins	Internet access	No impact
	Internet Services	30 mins	Email Services	No impact
Equipment malfunctions	Printer, Desk phone	30 mins	Printing Services	No impact
	Computer Laptop	1 hour	Video Conferencing	No impact

Emergency Communication Plan

Emergency Communications Plan		
Name	**Role**	**Phone & Address**
Venkat Potapragada	Executive Director of IT & Resources	+1-703-223-3221 venkatp@tscti.com
Jagan Pkkirisankar	Executive Director of Policy & External Relations	+1-704-808-0503 jaganp@tscti.com
Anupom Mukherjee	Chief Information Security and Risk Officer	+1-703 349-2025 anupomm@tscti.com
Caroline Rist	HR Manager	+1-703-479-8222 caroline.rist@tscti.com
Isha Sharma	Office Admin Manager	+1-571-442-0572 isha.sharma@tscti.com
Reddy Bollineni	Director Emergency Management and Risk Assurance	+1-502-488-0162 reddy.bollineni@tscti.com
Methods of communication (Cell phone, social media, person-to-person)		
Method	**Person Responsible**	**Notes**
Cell Phone	HR Manager	Personal contact number
Social Media	HR Team	Contact info on the social media platform
Person-to-person	Receptionist	Direct number to reception

Business Continuity Plan

This is our plan of action following a disaster. By following this we will be able to keep our business in operation or return to operation as quickly as possible.

These are the critical business functions we need run our business:

Critical Function	Recovery Time Objective	Staff in Charge	Resources Needed	Backup Resources
Power Outage	30mins	Electrical Staff	UPS Setup	Backup UPS
Server disk faulty	30mins	IT Helpdesk	Disk	Cloud Portal
Outlook PST	30mins	IT Helpdesk	Backups restore	Cloud Portal
Printer faulty	30mins	IT Helpdesk	Printer Support	Standby Printer
Server/system slowness	30mins	IT Helpdesk	RAM	Cloud Portal

This is our backup location we will use if our primary offices are compromised:

Backup Location: Cloud Storage Portal

Address: Cloud Storage Portal

Phone number: +1-609-945-3413

Contacting: Name: IT Helpdesk

Preventative Measures

What are some proactive preventative measures we could take to mitigate risk?

Hazard	Preventative Measures
Avoidance	It eliminates any hazard that might harm the organization, its assets, or its stakeholders; and removes the chance that the risk might become a reality.
Loss prevention	It identifies and reduces risks that could result in losses from theft, fraud, accidents, or other sources. It seeks to identify threats and vulnerabilities, and use measures to mitigate the potential for losses
Loss reduction	Closely related to loss prevention, above, loss reduction tries to reduce the chance of an incident – but also tries to limit the potential damage when the threat does happen.
Separation	It involves dispersing key assets so that catastrophic events at one location affect the business only at that location.

4. Responsibilities

The CEO is the approval authority for the BCP Plan.

The Steering Committee and the BCP Team is responsible for the implementation, and maintenance of the BCP Plan and associated standards and guidelines.

Company management is accountable for ensuring that the BCP Plan and associated standards and guidelines are properly communicated and understood within their respective organizational units. Company management is also responsible for defining, approving, and implementing procedures in its organizational units and ensuring their consistency with the BCP Plan and associated standards and guidelines.

All individuals, groups, or organizations identified in the scope of this policy are responsible for familiarizing themselves and complying with the BCP Plan and associated standards and guidelines.

5. Policy Enforcement and Exception Handling

Failure to comply with the BCP Plan and associated standards, guidelines, and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the BCP Plan should be submitted to the Company Program Manager. Exceptions shall be permitted only on receipt of written approval from the Program Manager. The Program Manager will periodically report the current status to the Company CEO or its designee.

6. Review and Revision

The BCP Plan will be reviewed and revised in accordance with the **Business Resilience and BCP Policy.**

Recommended: ________________________

Signature

Pakkirisankar Jagannath

Program Manager

Approved: ____________________________

Signature

Anil Sharma

CEO