JULICA CERTIFICATE POLICY

Security Management

- Data Protection Policy
- Incident Response plan
- Risk Management Plan
- IT Security Policy
- Business Continuity Plan
- Disaster Recovery Plan
- Subscriber Agreement
- Hiring Policy

DATA PROTECTION POLICY

Data Protection Policy

1 Introduction

JULICA is the data controller and processor of the information provided for registration, application, training, and certification purposes, as well as support services.

As declared in our data protection policy, we are dedicated to and responsible for processing the information of our employees, customers, stakeholders, and other interested parties with full caution and confidentiality. This policy describes how we collect, store, handle and secure our data.

The rules outlined in this document any form of data, be them stored electronically, on paper, or on any other storage device.

2 Privacy Elements

As part of our operations, we gather and process information or data that can make individuals identifiable, including, but not limited to, full name, phone number, account credentials, and home address.

The use of personal data by JULICA is governed by the Data Protection Act of Kenya, European General Data Protection Regulation (EU-GDPR), and other national privacy legislation that offer the same level of data protection as the GDPR.

We are committed to process all personal data under our control in accordance with data protection principles.

The data we process data will be:

- Processed in a lawful, fair, and transparent manner
- Collected only for specific, explicit, and limited purposes (purpose limitation)
- Adequate, relevant, and not excessive (data minimization)
- Accurate and kept up-to-date, where necessary
- Kept for no longer than necessary (retention)
- Handled with appropriate security and confidentiality

3 Roles and Responsibilities

All JULICA employees and collaborators are responsible for ensuring that the collection, storage, handling, and protection of data is done appropriately. The contact details of our Data Protection Officer are:

Person: Data Protection Officer

Email: Christina Wanjiku wood
Phone: +254795289184

The following are the responsibilities of specific people or departments:

3.1 Data Protection Officer

- Inform and advise the controller or processor and their employees of their obligations under data protection laws
- Act as a contact point for requests from individuals regarding the processing of their personal data and the exercise of their rights
- Oversee and implement data protection strategies
- Conduct regular assessments and audits to ensure GDPR compliance

3.2. Information Security Manager

- Oversee and improve cybersecurity awareness programs and risk management regularly
- Collaborate with the Security Committee in leading the design, implementation, operation, and maintenance of the information security management system.
- Ensure periodic testing are conducted to evaluate the security posture of information security
- Lead the design and operation of related compliance monitoring and improvement activities to ensure compliance both with internal security policies and applicable laws and regulations
- Develop and manage controls to ensure compliance with the requirements of various security laws, standards, and regulations

3.3. IT Systems Manager

- Strictly comply with all JULICA CA policies related to non-disclosure, non-competition, and the confidentiality of information
- Constantly stay up to date on various web technologies and tools
- Perform networking systems hardware and software upgrades and install security patches, as needed
- Check and monitor the general health of networks and networking devices
- Perform daily system monitoring, verify the integrity and availability of all hardware, server resources, systems, and IT processes, review system and application logs, and verify completion of scheduled jobs such as backups
- Implement, configure, and maintain computer networks, software, and digital security

3.4. Compliance Department

- Ensure that access to the personal data of Certification holders, Trainers, Examiners, Examinees, and Invigilators will not be shared with or provided to unauthorized parties
- Additional documents and data provided by applicants are being stored appropriately and centralized to ensure the confidentiality, integrity, availability of the data

3.5. Business Development Department

Ensure that access to JULICA Authorized users and Agents' personal data:

- Is restricted to authorized personnel only
- Will not be shared with or provided to unauthorized parties

3.6. System Administrator

Ensure that access to the personal data of members registered on the JULICA Website:

- Is restricted to authorized personnel only
- Will not be shared with or provided to unauthorized parties

4 General Guidelines

- Personal data of stakeholders shall be restricted only to employees who need it to complete their job in line with their job responsibilities.
- Informally sharing data is prohibited. When access to confidential information is needed, employees shall request it from their immediate superior.
- All JULICA CA employees shall undergo comprehensive training to help them understand their responsibilities when handling personal data.
- Data in the process by employees shall be kept secure and stored following the data storage guidelines presented in the chapter below.
- In particular, account credentials and passwords shall be kept in encrypted storage with restricted access.
- Personal data shall not be disclosed or communicated to unauthorized people, either within the company or externally.
- When unsure about any aspect of data protection, employees shall request assistance from their immediate superior or the Data Protection Officer.

5 Data Storage

These rules describe the storage and the process of safely storing data. Data is stored electronically shall be limited to authorized personnel only. The guideline also applies to electronically stored data printed out for specific reasons.

- Employees with access to electronic files shall ensure confidentiality.

Data shall be protected from unauthorized access, accidental deletion, and malicious hacking attempts.

- Data shall be protected with strong passwords that are changed regularly and never shared between employees.
- Data shall not be stored on removable media (like a CD or DVD). If necessary for job purposes, removable media shall be kept locked and secure.
- Data shall only be stored on designated servers at JULICA premises and shall only be uploaded onto approved cloud computing services.
- Servers containing personal data shall be sited in a secure location where access is restricted to authorized personnel only. The site must be monitored and access-controlled.
- Data shall be backed up daily. Backups shall be tested regularly, in line with the company's standard backup procedures.
- Data shall never be saved directly to laptops or other mobile devices (e.g., tablets or smartphones).
- All servers and computers containing data shall be protected by approved security software and a firewall.
- All data entering JULICA systems and website are stored as unique and measures to prevent privilege escalation are taken.
- All data entering into the database of the JULICA website are protected with certificates that ensure encrypted communication when receiving and sending information.

6 Data Usage

- All data collected by JULICA CA are strictly for JULICA-related services. They are used to provide complete responses or services. No other non-JULICA related service will be offered from the data collected.
- When working with personal data, employees shall ensure their computer screens are always locked when left unattended.
- Data shall be encrypted before being transferred electronically.
- Employees shall not save copies of personal data to their computers. Always access and update the central copy of any data.

7 Data Accuracy and Action

To exercise data protection, JULICA CA takes reasonable steps and is committed to:

- Restrict and monitor access to sensitive data
- Establish effective data collection procedures
- Provide employees with online privacy and security training
- Build secure networks to protect online data from cyberattacks
- Establish clear procedures for reporting privacy breaches or data misuse

- Include contract clauses or communicate statements on how we handle data
- Update the data continuously
- Ensure that marketing databases are checked against industry suppression files
- Install tracking logs to monitor employees' activities ensuring data is not being misused
- Install firewall and protection software that prevents employees from sharing and distributing data from JULICA CA devices externally by means of detecting large amounts of data being transferred via email or external drives
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization, etc.)

8 Subject Access Requests

All individuals and organizations who are subject of personal and other data held by JULICA are entitled to:

- Ask what information JULICA holds about them and why
- Ask how to gain access to it
- Be informed on how to keep it up to date
- Be informed on how the company meets its data protection obligations

Our clients can request such information directly through a subject access request made via email or through the digital form available here. We will always verify the identity of anyone making a subject access request before handing over any information.
Confirmation will be asked from the data subject using the email data subject used to register an account at JULICA. We aim to respond to the request within 14 days.

8.1 Data Modification

Our clients can request data modification or correction via email or through the digital form available. JULICA will verify the identity of anyone making a request before modifying or correcting any information.

8.2 Data Erasure

The data subject will be provided with all necessary information before erasure. Before proceeding with the erasure, the data subject will receive a statement from our Data Protection Officer explaining the outcome of the data being deleted. Erasure of data can be requested at any time.

9 Children

Our website is not intended for children or persons younger than 18. JULICA does not knowingly collect personally identifiable information (PII) of persons under the age of 18. We strive to comply with the provisions of The Data protection Act of Kenya and the European Union General Data Protection Regulation (EU GDPR). If you are a parent or

custodian of a child or person under 18 years old and you believe that they have provided us with information about themselves, please contact us

10 Disclosing data

In certain circumstances, when required, JULICA can disclose data to law enforcement agencies without the consent of the data subject. However, the data controller will ensure the request is lawful, seeking assistance from the board and from the company's legal advisors, where necessary.

11 Privacy Statement.

We have a privacy statement available on our website. It presents the type information we collect, the purpose of collection and use, third-party processors involved, and how we protect customers' data. The privacy statement is available at
https://tendaworld.com/policies/privacy/

INCIDENT RESPONSE PLAN

EXECUTIVE SUMMARY

To maintain the trust of our employees, customers, and partners and meet regulatory requirements, it is essential that we do everything we can to protect confidential information and systems in the face of a cyberattack. The better prepared we are to respond to a potential cyberattack, the faster we can eradicate any threat and reduce the impact on our business.

This document describes the plan for responding to information security incidents at JULICA. This document will explain how to detect and react to cybersecurity incidents and data breaches, determine their scope and risk, respond appropriately and quickly, and communicate the results and risks to all stakeholders.

Effective incident response involves every part of our organization, including IT teams, legal, technical support, human resources, corporate communications, and business operations. It is important that you read and understand your role as well as the ways you will coordinate with others.

This plan will be updated [at least annually] to reflect organizational changes, new technologies and new compliance requirements that inform our cybersecurity strategy. We will conduct regular testing of this plan to ensure everyone is fully trained to participate in effective incident response.

ROLES, RESPONSIBILITIES & CONTACT INFORMATION

This Security Incident Response Plan must be followed by all personnel, including all employees, temporary staff, consultants, contractors, suppliers and third parties operating on behalf of JULICA. All personnel are referred to as 'staff' within this plan.

Below are details about the roles and responsibilities of each member of JULICA to prevent and respond to a workplace incident. It is not an exhaustive list of duties but designed to give each employee a general understanding of their role and the roles of other employees in incident response and prevention.

Incident Response Team Responsibilities

The Incident Response Lead is responsible for:

- Making sure that the Security Incident Response Plan and associated response and escalation procedures are defined and documented. This is to ensure that the handling of security incidents is timely and effective.
- Making sure that the Security Incident Response Plan is current, reviewed and tested at least once each year.
- Making sure that staff with Security Incident Response Plan responsibilities are properly trained at least once each year.
- Leading the investigation of a suspected breach or reported security incident and initiating the Security Incident Response Plan when needed.
- Reporting to and liaising with external parties, including pertinent business partners, legal representation, law enforcement, etc., as is required.
- Authorizing on-site investigations by appropriate law enforcement or third-party security/forensic personnel, as required during any security incident investigation. This

includes authorizing access to/removal of evidence from site.

Security Incident Response Team (SIRT) members are responsible for:

- Making sure that all staff understand how to identify and report a suspected or actual security incident.
- Advising the Incident Response Lead of an incident when they receive a security incident report from staff.
- Investigating and documenting each reported incident.
- Taking action to limit the exposure of sensitive data and to reduce the risks that may be associated with any incident.
- Gathering, reviewing, and analysing logs and related information from various central and local safeguards, security measures and controls.
- Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.
- Assisting law enforcement during the investigation processes.This includes any forensic investigations and prosecutions.
- Initiating follow-up actions to reduce likelihood of recurrence, as appropriate.
- Determining if policies, processes, technologies, security measures or controls need to be updated to avoid a similar incident in the future. They also need to consider whether additional safeguards are required in the environment where the incident occurred.

All staff members are responsible for:

- Making sure they understand how to identify and report a suspected or actual security incident.
- Reporting a suspected or actual security incident to the Incident Response Lead (preferable) or to another member of the Security Incident Response Team (SIRT).
- Reporting any security related issues or concerns to line management, or to a member of the SIRT.
- Complying with the security policies and procedures of JULICA CA.

Roles, Responsibilities and Contact Information

[Below is a list of roles within an organization required to conduct a comprehensive, coordinated incident response. You should customize this list to match the size, structure, and regulatory and industry requirements of your organization. Include contact information for everyone involved in incident response, both internally and externally. You should keep a hardcopy of your incident response plan and contact information accessible.

ROLE	RESPONSIBILITY	CONTACT DETAILS
INFORMATION SECURITY		
CSO / CISO	Strategic lead. Develops technical, operational, and financial risk ranking criteria used to prioritize incident response plan. Authorizes when and how incident details are reported. Main point of contact for executive team and Board of Directors.	Name: Chris Daniels Phone: +254795289184 Email: mail@tenda.world
Incident Response Team Lead and Team Members	Central team that authorizes and coordinates incident response across multiple teams and functions through all stages of a cyber incident. Maintains incident response plan, documentation, and catalog of incidents. Responsible for identifying, confirming, and evaluating extent of incidents. Conducts random security checks to ensure readiness to respond to a cyberattack.	Name: Chris Daniels Phone: +254721138882 Email: mail@tenda.world
Identity and Access Team Lead and Team Members	Responsible for privilege management, enterprise password protection and role-based access control. Discovers, audits, and reports on all privilege usage. Conducts random checks to audit privileged accounts, validate whether they are required, and re-authenticate those that are. Monitors privileged account uses and proactively checks for indicators of	Name: Chris Daniels Phone: +254721138882 Email: mail@tenda.world

	compromise, such as excessive logins, or other unusual behavior. Informs incident response team of potential attacks that compromise privileged accounts, validates and reports on the extent of attacks. Takes action to prevent the spread of a breach by updating privileges.	
IT Operations and Support (internal)	Manages access to systems and applications for internal staff and partners. Centrally manages patches, hardware and software updates, and other system upgrades to prevent and contain a cyberattack.	Name Phone Email
Technical Partners (ISP, MSP, Hosting, Testing Partners, etc.) Third Party External Incident Response Teams	Manages security controls to limit the progression of a cyberattack across third-party systems and organizations. Coordinates with Internal Response Team to manage risks. Professional Incident response teams help ensure a solid Incident Response process is followed. It is highly recommended that the company identify and prepare an External Response Team that can be available in an emergency IR situation and provide any requested information prior to an emergency to help them become familiar with your environment.	Name: Chris Daniels Phone: +254795289184 Email: mail@tenda.world Name: Chris Daniels Phone:+254721138882 Email: mail@tenda.world
COMPLIANCE		
Legal Counsel	Confirms requirements for informing employees, customers,and the public about cyber breaches. Responsible for checking in with local law enforcement.	Name: Christina Wanjiku Wood Phone: +254795289184 Email: mail@tenda.world

	Ensures IT team has legal authority for privilege account monitoring.	
Audit & Compliance	Communicates with regulatory bodies, following mandated reporting requirements.	Name: Christina Wanjiku Wood Phone: +254795289184 Email: mail@tenda.world
Human Resources	Coordinates internal employee communications regarding breaches of personal information and responds to questions from employees.	Name: Christina Wanjiku Wood Phone: +254795289184 Email: mail@tenda.world
Regulatory Contacts	Receives information about a breach according to timeline and format mandated by regulatory requirements.	Name: Chris Daniels Phone: +254721138882 Email: mail@tenda.world
COMMUNICATIONS		
Marketing & Public Relations Lead	Communicates externally with customers, partners, and the media. Coordinates all communications and request for interviews with internal subject matter experts and security team. Maintains draft crisis communications plans and statements which can be customized and distributed quickly in case of a breach.	
Web & Social Media Lead	Posts information on the company website, email, and social media channels regarding the breach, including our response and recommendations for users. Sets up monitoring across social media channels to ensure we receivefeedback or questions sent by customers through social media.	
Technical Support Lead (Internal)	Provides security bulletins and technical guidance to employees in case of a breach, including required software updates, password changes, or other system changes.	Name: Chris Daniels Phone: +254721138882 Email: mail@tenda.world

TechnicalSupport Lead (External)	Provides security bulletins and technical guidance to external users in case of a breach.	Name: Chris Daniels Phone: +254795289184 Email: mail@tenda.world

Testing and Updates

[Annual] testing of the Incident Response Plan using walkthroughs and practical simulations of potential incident scenarios is necessary to ensure the SIRT are aware of their obligations, unless real incidents occur which test the full functionality of the process.

1. The Incident Response Plan will be tested [at least once annually].
2. The Incident Response Plan Testing will test [your business]'s response to potential incident scenarios to identify process gaps and improvement areas.
3. The SIRT will record observations made during the testing, such as steps that were poorly executed or misunderstood by participants and those aspects that need improvement.
4. The Incident Response Lead will ensure the Security Incident Response Plan is updated and distributed to SIRT members.

INCIDENT RESPONSE PROCESS OVERVIEW

1. Preparation—review and codify an organizational security policy, perform a risk assessment, identify sensitive assets, define which are critical security incidents the team should focus on, and build a Computer Security Incident Response Team (CSIRT).
2. Identification—monitor IT systems and detect deviations from normal operations and see if they represent actual security incidents. When an incident is discovered, collect additional evidence, establish its type and severity, and document everything.
3. Containment—perform short-term containment, for example by isolating the network segment that is under attack. Then focus on long-term containment, which involves temporary fixes to allow systems to be used in production, while rebuilding clean systems.
4. Eradication—remove malware from all affected systems, identify the root cause of the attack, and take action to prevent similar attacks in the future.
5. Recovery—bring affected production systems back online carefully, to prevent additional attacks. Test, verify and monitor affected systems to ensure they are back to normal activity.
6. Lessons learned—no later than two weeks from the end of the incident, perform a retrospective of the incident. Prepare complete documentation of the incident, investigate the incident further, understand what was done to contain it and whether anything in the incident response process could be improved.

Incident Response Checklist

To demonstrate and improve the effectiveness of JULICA CA incident response team and security tools, JULICA CA requires a record of all actions taken during each phase of an incident. Supporting documentation is required, including all forensic evidence collected such as activity logs, memory dumps, audits, network traffic, and disk images.

PHASE OF CYBER INCIDENT	ACTION	TEAM MEMBER/SYSTEM	DAY/TIME ACTION TAKEN
Incident Discovery and Confirmation	Describe how the team first learned of the attack (security researcher, partner, employee, customer, auditor, internal security alert, etc.).		
	Analyze audit logs and security applications to identify unusual or suspicious account behavior or activities that indicate a likely attack and confirm attack has occurred.		
	Describe potential attacker, including known or expected capabilities, behaviors, and motivations.		
	Identify access point and source of attack (endpoint, application, malware downloaded, etc.) and responsible party.		
	Prepare an incident timeline to keep an ongoing record of when the attack occurred and subsequent milestones in analysis and response.		
	Check applications for signatures, IP address ranges, files hashes, processes, executables names, URLs, and domain names of known malicious websites.		
	Evaluate extent of damage upon discovery and risk to systems and privileged accounts. Audit which privileged accounts have been used recently, whether any passwords have been changed, and what applications have been executed.(See Appendix A for more information on Threat Classification).		

	Review your information assets list to identify which assets have been potentially compromised.Note integrity of assets and evidence gathered. (See Appendix A for more information on Threat Classification).		
	Diagram the path of the incident/attack to provide an "at-a-glance" view from the initial breach to escalation and movement tracked across the network.		
	Collect meeting notes in a central repository to use in preparing communications with stakeholders.		
	Inform employees regarding discovery.		
	Analyze incident Indicators of Compromise (IOCs) with threat intelligence tools.		
	Potentially share information externally about breach discovery. You may choose to hold communications during this phase until you have contained the breach to increase your chances of catching the attacker. If so, make sure this aligns with your compliance requirements.		
Containment and Continuity	Enable temporary privileged accounts to be used by the technical and security team to quickly access and monitor systems.		
	Protect evidence. Back up any compromised systems as soon as possible, prior to performing any actions that could affect data integrity on the original media.		
	Force multi-factor authentication or peer review to ensure privileges are being used appropriately.		
	Change passwords for all users, service, application, and network accounts.		
	Increase the sensitivity of application security controls (allowing, denying, and restricting) to prevent malicious malware from being distributed by the attacker.		
	Remove systems from production or take systems offline if needed.		

	Inform employees regarding breach containment.		
	Analyze, record, and confirm any instances of potential data exfiltration occurrences across the network.		
	Potentially share information externally regarding breach containment (website updates, emails, social media posts, tech support bulletins, etc.).		
Eradication	Close firewall ports and network connections.		
	Test devices and applications to be sure any malicious code is removed.		
	Compare data before and after the incident to ensure systems are reset properly.		
	Inform employees regarding eradication.		
	Potentially share information externally regarding eradication (website updates, emails, social media posts, tech support bulletins, etc.).		
Recovery	Download and apply security patches.		
	Close network access and reset passwords.		
	Conduct vulnerability analysis.		
	Return any systems that were taken offline to production.		
	Inform employees regarding recovery.		
	Share information externally regarding recovery (website updates, emails, social media posts, tech support bulletins, etc.).		
Lessons Learned	Review forensic evidence collected.		
	Assess incident cost.		
	Write an Executive Summary of the incident.		
	Report to executive team and auditors if necessary.		
	Implement additional training for everyone involved in incident response and all employees.		
	Update incident response plan.		
	Inform employees regarding lessons learned, additional training, etc.		

Document Name:	Security Incident Response Plan
Current Version:	
Plan Owner:	
Plan Approver:	
Date of Last Review:	

	Potentially share information externally (website updates, emails, social media posts, tech support bulletins, etc.).		

Responsibilities At-a-Glance

Activity	Role				
	CSIRT Incident Lead	IT Contact	Legal Representative	Communications Officer	Management
Initial Assessment	Owner	Advises	None	None	None
Initial Response	Owner	Implements	Updates	Updates	Updates
Collects Forensic Evidence	Implements	Advises	Owner	None	None
Implements Temporary Fix	Owner	Implements	Updates	Updates	Advises
Sends Communication	Advises	Advises	Advises	Implements	Owner
Check with Local Law Enforcement	Updates	Updates	Implements	Updates	Owner
Implements Permanent Fix	Owner	Implements	Updates	Updates	Updates
Determines Financial Impact on Business	Updates	Updates	Advises	Updates	Owner

Document Control

THREAT CLASSIFICATION

The CIA Triad (Confidentiality, Integrity, and Availability) is a framework for incident classification that helps to prioritize the level of incident response required for a cyberattack.

1. Confidentiality – Incidents involving unauthorized access to systems, including privileged account compromise. The more confidential the data or the more important the systems are to the business, the higher the potential impact.
2. Integrity – Incidents involving data poisoning, including leveraging a privileged account to

corrupt or modify data. The more sensitive the data, the higher the potential impact.

3. Availability – Incidents that impact the availability or proper functioning of services, such as Distributed Denial of Service (DDoS) or ransomware, including use of privileged accounts to make unauthorized changes. The more critical the services to the business, the higher the potential impact.

When ranking the level of risk to the organization and the type of incident response required, you must consider the extent to which privileged accounts are compromised, including those associated with business users, network administrators, and service or application accounts. When privileged accounts are involved in the breach, the level of risk increases exponentially as does the response required.

COMPLIANCE AND LEGAL OBLIGATIONS

EU GDPR

Any organization dealing with EU citizens' Personally Identifiable Information is obligated to meet standards for effective data protection, adequate security measures, and privacy by design to comply with EUGDPR.

- Reporting requirements – Under GDPR, breach notification is mandatory in all member states where a data breach is likely to result in a risk for the rights and freedoms of individuals. This must be done within 72 hours of first having become aware of the breach. Data processors are required to notify their customers, the controllers, without undue delay after first becoming aware of a data breach.
- Learn more – https://gdpr.eu/

RISK MANAGEMENT PLAN

INTRODUCTION

Purpose Of The Risk Management Plan

A risk is an event or condition that, if it occurs, could have a positive or negative effect on a project's objectives. Risk Management is the process of identifying, assessing, responding to, monitoring, and reporting risks. This

Risk Management Plan defines how risks associated with the JuliCA project will be identified, analyzed, and managed. It outlines how risk management activities will be performed, recorded, and monitored throughout the lifecycle of the project and provides templates and practices for recording and prioritizing risks.
The Risk Management Plan is created by the project manager in the Planning Phase of the CDC Unified Process and is monitored and updated throughout the project.
The intended audience of this document is the project team, project sponsor and management.

Risk management Procedure

Process

The project manager working with the project team and project sponsors will ensure that risks are actively identified, analyzed, and managed throughout the life of the project. Risks will be identified as early as possible in the project so as to minimize their impact. The steps for accomplishing this are outlined in the following sections. The <project manager or other designee> will serve as the Risk Manager for this project.

Risk Identification

Risk identification will involve the project team, appropriate stakeholders, and will include an evaluation of environmental factors, organizational culture and the project management plan including the project scope. Careful attention will be given to the project deliverables, assumptions, constraints, WBS, cost/effort estimates, resource plan, and other key project documents.
A Risk Management Log will be generated and updated as needed and will be stored electronically in the project library located at <file location>.

Risk Analysis

All risks identified will be assessed to identify the range of possible project outcomes. Qualification will be used to determine which risks are the top risks to pursue and respond to and which risks can be ignored.

Qualitative Risk Analysis

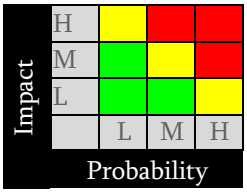
The probability and impact of occurrence for each identified risk will be assessed by the project manager, with input from the project team using the following approach:

Probability

- High – Greater than <70%> probability of occurrence.
- Medium – Between <30%> and <70%> probability of occurrence
- Low – Below <30%> probability of occurrence

Impact

- High – Risk that has the potential to greatly impact project cost, project schedule or performance
- Medium – Risk that has the potential to slightly impact project cost, project schedule or performance
- Low – Risk that has relatively little impact on cost, schedule or performance



Risks that fall within the RED and YELLOW zones will have risk response planning which may include both a risk mitigation and a risk contingency plan.

Quantitative Risk Analysis

Analysis of risk events that have been prioritized using the qualitative risk analysis process and their affect on project activities will be estimated, a numerical rating applied to each risk based on this analysis, and then documented in this section of the risk management plan.

Risk Response Planning

Each major risk (those falling in the Red & Yellow zones) will be assigned to a project team member for monitoring purposes to ensure that the risk will not "fall through the cracks".
For each major risk, one of the following approaches will be selected to address it:

- Avoid – eliminate the threat by eliminating the cause
- Mitigate – Identify ways to reduce the probability or the impact of the risk
- Accept – Nothing will be done
- Transfer – Make another party responsible for the risk (buy insurance, outsourcing, etc.)

For each risk that will be mitigated, the project team will identify ways to prevent the risk from occurring or reduce its impact or probability of occurring. This may include prototyping, adding tasks to the project schedule, adding resources, etc.
For each major risk that is to be mitigated or that is accepted, a course of action will be outlined for the event that the risk does materialize in order to minimize its impact.

Risk Monitoring, Controlling, And Reporting

The level of risk on a project will be tracked, monitored and reported throughout the project lifecycle.
A "Top 10 Risk List" will be maintained by the project team and will be reported as a component of the project status reporting process for this project.
All project change requests will be analyzed for their possible impact to the project risks.
Management will be notified of important changes to risk status as a component to the Executive Project Status Report.

Tools And Practices

A Risk Log will be maintained by the project manager and will be reviewed as a standing agenda item for project team meetings.

Risk management plan approval

The undersigned acknowledge they have reviewed the Risk Management Plan for the JuliCA project. Changes to this Risk Management Plan will be coordinated with and approved by the undersigned or their designated representatives.

Signature: _____ Date: _____

Print Name: _____

Title: _____

Role: _____

Signature: _____ Date: _____

Print Name: _____

Title: _____

Role: _____

Signature: _____ Date: _____

Print Name: _____

Title: _____

Role: _____

I.T. Security Policy

1. POLICY STATEMENT

"It shall be the responsibility of the I.T. Department to provide adequate protection and confidentiality of all corporate data and proprietary software systems, whether held centrally, on local storage media, or remotely, to ensure the continued availability of data and programs to all authorised members of staff, and to ensure the integrity of all data and configuration controls."

Summary of Main Security Policies.

1.1 Confidentiality of all data is to be maintained through discretionary and mandatory access controls, and wherever possible these access controls should meet with C2 class security functionality.

1.2 Internet and other external service access is restricted to authorised personnel only.

1.3 Access to data on all laptop computers is to be secured through encryption or other means, to provide confidentiality of data in the event of loss or theft of equipment.

1.4 Only authorised and licensed software may be installed, and installation may only be performed by I.T. Department staff.

1.5 The use of unauthorised software is prohibited. In the event of unauthorised software being discovered it will be removed from the workstation immediately.

1.6 Data may only be transferred for the purposes determined in the Organisation's data-protection policy.

1.7 All diskette drives and removable media from external sources must be virus checked before they are used within the Organisation.

1.8 Passwords must consist of a mixture of at least 8 alphanumeric characters, and must be changed every 40 days and must be unique.

1.9 Workstation configurations may only be changed by I.T. Department staff.

1.10 The physical security of computer equipment will conform to recognised loss prevention guidelines.

1.11 To prevent the loss of availability of I.T. resources measures must be taken to backup data, applications and the configurations of all workstations.

1.12 A business continuity plan will be developed and tested on a regular basis.

2. VIRUS PROTECTION

2.1 The I.T. Department will have available up to date virus scanning software for the scanning and removal of suspected viruses.
2.2 Corporate file-servers will be protected with virus scanning software.
2.3 Workstations will be protected by virus scanning software.
2.4 All workstation and server anti-virus software will be regularly updated with the latest anti-virus patches by the I.T. Department.
2.5 No disk that is brought in from outside the Organisation is to be used until it has been scanned.
2.6 All systems will be built from original, clean master copies whose write protection has always been in place. Only original master copies will be used until virus scanning has taken place.
2.7 All removable media containing executable software (software with .EXE and .COM extensions) will be write protected wherever possible.
2.8 All demonstrations by vendors will be run on their machines and not the Organisation's.
2.9 Shareware is not to be used, as shareware is one of the most common infection sources. If it is absolutely necessary to use shareware it must be thoroughly scanned before use.
2.10 New commercial software will be scanned before it is installed as it occasionally contains viruses.
2.11 All removable media brought in to the Organisation by field engineers or supportpersonnel will be scanned by the IT Department before they are used on site.
2.12 To enable data to be recovered in the event of a virus outbreak regular backups will be taken by the I.T. Department.
2.13 Management strongly endorse the Organisation's anti-virus policies and will make the necessary resources available to implement them.
2.14 Users will be kept informed of current procedures and policies.

2.15 Users will be notified of virus incidents.

2.16 will be accountable for any breaches of the Organisation's anti-virus policies.

2.17 Anti-virus policies and procedures will be reviewed regularly.

In the event of a possible virus infection the user must inform the I.T. Department immediately. The I.T. Department will then scan the infected machine and any removable media or other workstations to which the virus may have spread and eradicate it.

3. PHYSICAL SECURITY OF COMPUTER EQUIPMENT

Physical Security of computer equipment will comply with the guidelines as detailed below.

3.1 DEFINITIONS

3.1.1. AREA

Two or more adjacent linked rooms which, for security purposes, cannot be adequately segregated in physical terms.

3.1.2. COMPUTER SUITE

Mainframe, minicomputer, fileserver plus all inter-connected wiring, fixed disks, telecommunication equipment, ancillary, peripheral and terminal equipment linked into the mainframe, contained within a purpose built computer suite.

3.1.3. COMPUTER EQUIPMENT

All computer equipment not contained within the COMPUTER SUITE which will include PC's, monitors, printers, disk drives, modems and associated and peripheral equipment.

3.1.4. HIGH RISK SITUATION(S)

This refers to any room or AREA which is accessible

- at ground floor level
- at first floor level, but accessible from adjoining roof
- at any level via external fire escapes or other features providing access
- rooms in remote, concealed or hidden areas

3.1.5. LOCKDOWN DEVICE(S)

A combination of two metal plates, one for fixing to furniture, or the building structure, and the other for restraining the equipment which is immobilised when the two plates are locked together. The plate for restraining the equipment should incorporate an enclosure or other mechanism which will hinder unauthorised removal of the outer PC casing and render access to internal components difficult.

3.1.6. APPROVED

Approved security system.

3.1.7. PERSONAL COMPUTERS (PC's)

Individual computer units with their own internal processing and storage capabilities.

3.2 CATEGORIES OF RISK

3.2.1. SECURITY LEVEL 1:	the security measures detailed in Level 1 are guidelines for all COMPUTER EQUIPMENT not described below.
3.2.2. SECURITY LEVEL 2:	these guidelines apply where a single room or AREA contains PC's where the total replacement value of this hardware is LESS than 20,000 per room or AREA.
3.2.3. SECURITY LEVEL 3:	these guidelines apply where a single room or AREA contains PC's where the total replacement value of this hardware is between 20,000 and 50,000 per room or AREA.
3.2.4. SECURITY LEVEL 4:	these guidelines apply where a single room or AREA contains PC's where the total replacement value of this hardware is in excess of 50,000 per room or AREA.

3.2.5. COMPUTER SUITE

These guidelines apply to the location or room comprising the purpose built computer suite.

3.3 REQUIRED PHYSICAL SECURITY

The table below summarises the required features for each Security Level.

No	Security Features	Security Level			
		1	2	3	4
1	Security Marking	x	x	x	x
2	Locking of PC cases	x	x	x	x
3	Siting of computers away from windows	x	x	x	x
4	HIGH RISK SITUATION window locks	x	x	x	N/A
5	Blinds for observable windows	x	x	x	x
6	If no intruder alarm, all PC's and COMPUTER EQUIPMENT> 1,500, to have a LOCKDOWN DEVICE	x	x	N/A	N/A
7	Intruder alarm installed by APPROVED Company		x	x	x
8	Protection of signal transmission to Alarm Receiving Centre		x	N/A	N/A
9	Assessment of location of intruder alarm protection		x	x	x
10	Walk test of movement detectors		x	x	x
11	Check that movement detectors are not obscured		x	N/A	N/A
12	Anti-masking intruder alarm sensors in room or AREA			x	N/A
13	Break glass alarm sensors			x	x
14	Individual alarm zoning of the room or AREA			x	N/A
15	Improved protection of signal transmission to Alarm Receiving Centre			x	N/A
16	Minimum room or AREA construction			x	N/A
17	Door specification for entry to room or AREA			x	x
18	Anti-masking intruder alarm sensors in room and access routes				x
19	Alarm shunt lock on door				x
20	Visual or audio alarm confirmation				x
21	Superior protection of alarm signal transmission				x
22	Improved room or AREA construction				x
23	All external opening windows to have locks				x
24	HIGH RISK SITUATION windows to have shutters/bars				x

Where an entry is shown as N/A (not applicable) this is due to a higher specification being required thereby removing the necessity for the lower security feature.

3.3.1. Security Marking

All computer hardware should be prominently security marked by branding or etching with the name of the establishment and area postcode. Advisory signs informing that all property has been security marked should be prominently displayed externally. The following are considered inferior methods of security

marking; text comprised solely of initials or abbreviations, marking by paint or ultra violet ink (indelible or otherwise), or adhesive labels that do not include an etching facility.

3.3.2. Locking of PC cases

PC's fitted with locking cases will be kept locked at all times.

3.3.3. Siting of Computers

Wherever possible, COMPUTER EQUIPMENT should be kept at least

1.5 metres away from external windows in HIGH RISK SITUATIONS.

3.3.4. Opening Windows

All opening windows on external elevations in HIGH RISK SITUATIONS should be fitted with key operated locks.

3.3.5. Blinds

All external windows to rooms containing COMPUTER EQUIPMENT at

ground floor level or otherwise visible to the public should be fitted with window blinds or obscure filming.

3.3.6. Lockdown Devices

For any item of COMPUTER EQUIPMENT with a purchase price in

excess of 1,500 which is not directly covered by an intruder alarm, the processing unit should have a LOCKDOWN DEVICE fitted to the workstation. LOCKDOWN DEVICES should conform to loss prevention standards.

Mobile workstations are unlikely to be suitable for these devices.
When it is impossible or undesirable to anchor hardware, such equipment can be moved to a security store or cabinet outside normal hours of occupation.

3.3.7. Intruder Alarm

An intruder alarm incorporating the following features should be installed. Installation, maintenance and monitoring by an APPROVED company.

3.3.8. Protection of Signal Transmission

Unless telephone wires directly enter the protected premises underground, signalling to the Alarm Receiving Centre should be by direct line.

3.3.9. Location of Intruder Alarms

Detection devices should be located within the room or AREA and elsewhere in the premises to ensure that unauthorised access to the room or AREA is not possible without detection. This should include an assessment as to whether access is possible via external elevations, doors, windows and rooflights.

3.3.10. Walktest

A walk test of movement detectors should be undertaken on a regular basis in order to ensure that all PC's are located within the alarmprotected area. This is necessary due to the possible ongoing changes

in the position of furniture, screens and partitions, which may seriously impede the field of cover provided by existing detection devices. For any PC which is not directly covered by an intruder alarm, the processing unit should have a LOCKDOWN DEVICE.

3.3.11. Check Detectors

Building managers should ensure, as part of their normal duties at locking up time, that

internal space detectors have not been individually obscured or had their field of vision restricted.

3.3.12. Anti-Masking Intruder Alarm

Anti-masking intruder alarm movement sensors are recommended to immediately detect a movement within the room or AREA.

3.3.13. Break Glass Alarm Sensors

Break Glass alarm sensors to detect forced entry through external windows of the room or AREA are recommended.

3.3.14. Alarm Zoning

The ability to zone the intruder alarm from the main control panel should be provided to enable authorised usage of other areas of the building outside normal hours, whilst retaining alarm detection within the room or AREA.

3.3.15. Improved Protection of Signal Transmission

Unless telephone wires directly enter the protected premises underground, signalling to the Alarm Receiving Centre should be by monitored direct line.

3.3.16. AREAConstruction

Partitions separating the room or AREA from adjoining rooms and corridors should be a minimum of 100mm solid non lightweight blockwork or brickwork devoid of glazing or other openings except for protected doors as defined below. If glazing is essential for lighting or other purposes, it should be upgraded by being supplemented internally with 1.5mm mesh, security shutters or bars or supplemented with 7.5mm laminated glass.

3.3.17. Door Specification

All doors giving access to the room or AREA both from within and outside the building, should be, as a minimum, solid timber and at least 45mm thick, preferably unglazed. Doors should have a mortise deadlock with key registration. Door fittings should comprise 3 hinges, supplemented by 2 hinge bolts if outward opening. Inward opening doors to the room or AREA should have a London bar (a metal strip strengthening the locking post of the door frame).

Where a door is glazed as a fire requirement, and entry is either possible through the glazing (where the width or height of the glazing exceeds 200mm in either direction) or by breaking the glazing to reach

an internal release mechanism, the glazing should be supplemented internally with 1.5mm, or 7.5mm laminated glass, retaining the wired glass for fire resistance.

3.3.18. Intruder Alarm Sensors on Access Routes

Anti-masking intruder alarm movement sensors are recommended to immediately detect a movement within the room or AREA and any internal corridors or rooms giving access to the room or AREA.

3.3.19. Alarm Shunt Lock

The alarm should have the facility for setting and unsetting within the room or AREA independently of the status of the main premises control panel via a shunt lock on the room or AREA access door. It should not be possible to set the main system if the room or AREA detection is 'shunted out'.

3.3.20. Alarm Confirmation

Visual or audio alarm confirmation should be provided at the monitoring facility for all conventional detection within the room or AREA.

3.3.21. Superior Protection of Signal Transmission

Monitored signalling to the Alarm Receiving Centre should be either by direct line or use monitoring service.

3.3.22. Improved AREA Construction

Partitions separating the room or AREA from adjoining rooms and corridors should be a minimum of 150mm solid non lightweight blockwork or brickwork devoid of glazing or other openings except for protected doors as defined below. Where glazing is essential for lighting or other purposes this should be protected by security shutters or bars .

Secure doors giving access to the room or AREA, from within the building, should be solid timber at least 45mm thick and unglazed. The locking should be by 2 mortise deadlocks to with registered keys, a micro switch being available for an alarm shunt lock. Door fittings should comprise 3 hinges, supplemented by 2 hinge bolts if outward opening doors. Inward opening doors to room or AREA should have a London bar (a metal strip strengthening the locking post of the door frame).

3.3.23. External Windows to Have Locks

All opening windows within the perimeter of the room or AREA should be fitted with key-operated window locks.

3.3.24. HIGH RISK SITUATIONS

Where the room or AREA is classified as being in a HIGH RISK SITUATION the following additional protection should be provided.

Windows to external elevations should be fitted with security shutters or bars instead of locks.

Any door in the external elevation should be provided with a security shutter where practical. Considerations should be given to replacement of fire exit doors which cannot be secured in this fashion, and any other doors designated as fire escapes by the Fire Prevention Officer, with proprietary security doors and frames fitted with a four point locking bolt and an alarm vibration sensor.

3.4 COMPUTER SUITE

3.4.1. The computer suite should be housed in a purpose built room.

3.4.2. Partitions separating the room or AREA from adjoining rooms and corridors should be a minimum of 150mm solid non lightweight blockwork or brickwork devoid of glazing or other openings except for protected doors as defined below. Where glazing is essential for lighting or other purposes this should be protected by bars.

3.4.3. Secure doors giving access to the room or AREA, from within the building, should be solid timber at least 45mm thick and unglazed. The locking should be by 2 mortise deadlocks with registered keys, a micro switch being available for an alarm shunt lock. Door fittings should comprise 3 hinges, supplemented by 2 hinge bolts if outward opening doors. Inward opening doors to room or AREA should have a London bar (a metal strip strengthening the locking post of the door frame). The computer suite should contain an adequate air conditioning system to provide a stable operating environment to reduce the risk of system crashes due to component failure.

3.4.4. No water, rain water or drainage pipes should run within or above the computer suite to reduce the risk of flooding.

3.4.5. The floor within the computer suite should be a raised false floor to allow

computer cables to run beneath the floor and reduce the risk of damage to computer equipment in the case of flooding.

3.4.6. Power points should be raised from the floor to allow the smooth shutdown of computer systems in case of flooding.

3.4.7. Where possible generator power should provided to the computer suite to help protect the computer systems in the case of a mains power failure.

3.4.8. All contractors working within the computer suite are to be supervised at all times and the It Department is to be notified of their presence and provided with details of all work to be carried out, at least 48 hours in advance of its commencement.

4. ACCESS CONTROL

4.1 Users will only be given sufficient rights to all systems to enable them to perform their job function. User rights will be kept to a minimum at all times.

4.2 Users requiring access to systems must make a written application on the forms provided by the I.T Department.

4.3 Where possible no one person will have full rights to any system. The I.T. Department will control network/server passwords and system passwords will be assigned by the system administrator in the enduser department. The system administrator will be responsible for the maintaining the data integrity of the end-user department's data and for determining end-user access rights.

4.4 Access to the network/servers and systems will be by individual username and password, or by smartcard and PIN number/biometric.

4.5 Usernames and passwords must not be shared by users.

4.6 Usernames and passwords should not be written down.

4.7 Usernames will consist of initials and surname.

4.8 All users will have an alphanumeric password of at least 8 characters.

4.9 Passwords will expire every 40 days and must be unique.

4.10 Intruder detection will be implemented where possible. The user account will be locked after 3 incorrect attempts.

4.11 The I.T. Department will be notified of all employees leaving the Organisation's employment. The I.T. Department will then remove the employees rights to all systems.

4.12 Network/server supervisor passwords and system supervisor passwords will be stored in a secure location in case of an emergency or disaster, for example a fire safe in the I.T. Department.

4.13 Auditing will be implemented on all systems to record login attempts/failures, successful logins and changes made to all systems.

4.14 I.T. Department staff will not login as root on to UNIX, Linux systems, but will use the su command to obtain root privileges.

4.15 Use of the admin username on Novell systems and the Administrator username on Windows is to be kept to a minimum.

4.16 Default passwords on systems such as Oracle and SQLServer will be changed after installation.

4.17 On UNIXand Linux systems, rights to rlogin, ftp, telnet, ssh will be restricted to

4.18 I.T. Department staff only.

4.19 Where possible users will not be given access to the UNIX, or Linux shell prompt.

4.20 Access to the network/servers will be restricted to normal working hours. Users requiring access outside normal working hours must request such access in writing on the forms provided by the I.T. Department.

4.21 File systems will have the maximum security implemented that is possible. Where possible users will only be given Read and Filescan rights to directories, files will be flagged as read only to prevent accidental deletion.

5. LAN Security

Hubs & Switches

5.1 LAN equipment, hubs, bridges, repeaters, routers, switches will be kept in secure hub rooms. Hub rooms will be kept locked at all times. Access to hub rooms will be restricted to I.T. Department staff only. Other staff, and contractors requiring access to hub rooms will notify the I.T. Department in advance so that the necessary supervision can be arranged.

Workstations

5.2 Users must logout of their workstations when they leave their workstation for any length of time. Alternatively Windowsworksations may be locked.

5.3 All unused workstations must be switched off outside working hours.

Wiring

5.4 All network wiring will be fully documented.

5.5 All unused network points will be de-activated when not in use.

5.6 All network cables will be periodically scanned and readings recorded for future reference.

5.7 Users must not place or store any item on top of network cabling.

5.8 Redundant cabling schemes will be used where possible.

Monitoring Software

5.9 The use of LAN analyser and packet sniffing software is restricted to the I.T. Department.

5.10 LAN analysers and packet sniffers will be securely locked up when not in use.

5.11 Intrusion detection systems will implemented to detect unauthorised access to the network

Servers

5.12 All servers will be kept securely under lock and key.

5.13 Access to the system console and server disk/tape drives will be restricted to authorised I.T. Department staff only.

Electrical Security

5.14 All servers will be fitted with UPS's that also condition the power supply.

5.15 All hubs, bridges, repeaters, routers, switches and other critical network equipment will also be fitted with UPS's.

5.16 In the event of a mains power failure, the UPS's will have sufficient power to keep the network and servers running until the generator takes over.

5.17 Software will be installed on all servers to implement an orderly shutdown in the event of a total power failure.

5.18 All UPS's will be tested periodically.

Inventory Management

5.19 The I.T. Department will keep a full inventory of all computer equipment and software in use throughout the Company.

5.20 Computer hardware and software audits will be carried out periodically via the use of a desktop inventory package. These audits will be used to track unauthorised copies of software and unauthorised changes to hardware and software configurations.

6. Server Specific Security

This section applies to Windows, UNIX, Linux and Novell servers.

6.1 The operating system will be kept up to date and patched on a regular basis.

6.2 Servers will be checked daily for viruses.

6.3 Servers will be locked in a secure room.

6.4 Where appropriate the server console feature will be activated.

6.5 Remote management passwords will be different to the Admin/Administrator/root password.

6.6 Users possessing Admin/Administrator/root rights will be limited to trained members of the I.T. Department staff only.

6.7 Use of the Admin/Administrator/root accounts will be kept to a minimum.

6.8 Assigning security equivalences that give one user the same access rights as another user will be avoided where possible.

6.9 Users access to to data and applications will be limited by the access control features.

6.10 Intruder detection and lockout will be enabled.

6.11 The system auditing facilities will be enabled.

6.12 Users must logout or lock their workstations when they leave their workstation for any length of time.

6.13 All unused workstations must be switched off outside working hours.

6.14 All accounts will be assigned a password of a minimum of 8 characters.

6.15 Users will change their passwords every 40 days.

6.16 Unique passwords will be used.

6.17 The number of grace logins will be limited to 3.

6.18 The number of concurrent connections will be limited to 1.

6.19 Network login time restrictions will be enforced preventing users from logging in to the network outside normal working hours.

6.5. In certain areas users will be restricted to logging in to specified workstation only.

7. UNIX & Linux Specific Security

7.1 Direct root access will be limited to the system console only.

7.2 I.T. Department staff requiring root access must make use of the su command.

7.3 Use of the root account will be kept to a minimum.

7.4 All UNIX and Linux system accounts will be password protected, lp etc.

7.5 rlogin facilities will be restricted to authorised I.T. Department staff only.

7.6 ftp facilities will be restricted to authorised I.T. Services staff only.

7.7 telnet facilities will be restricted to authorised users.

7.8 facilities will be restricted to authorised users.

7.9 Users access to data and applications will be limited by the access control features.

7.10 Users will not have access to the $ prompt.

7.11 All accounts will be assigned a password of a minimum of 8 characters.

7.12 Users will change their passwords every 40 days.

8. Wide Area Network Security

8.1 Wireless LAN's will make use of the most secure encryption and authentication facilities available.

8.2 Users will not install their own wireless equipment under any circumstances.

8.3 Dial-in modems will not be used if at all possible. If a modem must be used dial-back modems should be used. A secure VPN tunnel is the preferred option.

8.4 Modems will not be used by users without first notifying the I.T. Department and obtaining their approval.

8.5 Where dial-in modems are used, the modem will be unplugged from the telephone network and the access software disabled when not in use.

8.6 Modems will only be used where necessary, in normal circumstances all communications should pass through the Organisation's router and firewall.

8.7 Where leased lines are used, the associated channel service units will be locked up to prevent access to their monitoring ports.

8.8 All bridges, routers and gateways will be kept locked up in secure areas.

8.9 Unnecessary protocols will be removed from routers.

8.10 The preferred method of connection to outside Organisations is by a secure VPN connection, using IPSEC or SSL.

All connections made to the Organisation's network by outside organisations will be logged.

9. TCP/IP & Internet Security

9.1 Permanent connections to the Internet will be via the means of a firewall to regulate network traffic.

9.2 Permanent connections to other external networks, for offsite processing etc., will be via the means of a firewall to regulate network traffic.

9.3 Where firewalls are used, a dual homed firewall (a device with more than one TCP/IP address) will be the preferred solution.

9.4 Network equipment will be configured to close inactive sessions.

9.5 here modem pools or remote access servers are used, these will be situated on the DMZ or non-secure network side of the firewall.

9.6 Workstation access to the Internet will be via the Organisation's proxy server and website content scanner

9.7 All incoming e-mail will be scanned by the Organisation's e-mail content scanner.

10. Voice System Security

10.1 DISA port access (using inbound 0800 numbers) on the PBX will be protected by a secure password.

10.2 The maintenance port on the PBX will be protected with a secure password.

10.3 The default DISA and maintenance passwords on the PBX will be changed to user defined passwords.

10.4 Call accounting will be used to monitor access to the maintenance port, DISA ports and abnormal call patterns.

10.5 DISA ports will be turned off during non working hours.

10.6 Internal and external call forwarding privileges will be separated, to prevent inbound calls being forwarded to an outside line.

10.7 The operator will endeavour to ensure that an outside call is not transferred to an outside line.

10.8 Use will be made of multilevel passwords and access authentication where available on the PBX.

10.9 Voice mail accounts will use a password with a minimum length of six digits.

10.10 The voice mail password should never match the last six digits of the phone number.

10.11 The caller to a voice mail account will be locked out after three attempts at password validation.

10.12 Dialling calling party pays numbers will be prevented.

10.13 Telephone bills will be checked carefully to identify any misuse of the telephone system.

11. Glossary

Access Control	The process of limiting access to the resources of a system only to authorised programs, processes, or other systems.
Audit Trail	A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results.
Authenticate	To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.
Authorisation	The granting of access rights to a user, program, or process.
C2 Security	American security classification generally accepted world-wide, classifying the level of security provided.
CE	Products which meet the essential requirements of European Community directives for safety and protection carry this mark. Products which carry the CE mark may be sold anywhere in the community.

DISA	Direct inward system access. DISA is used to allow an inward-calling person access to an outbound line. Many PBXs have inbound 0800 numbers for employee use. Employees use them to retrieve their voice mail and to speak to people in the office.
Discretionary Access Control	A means of restricting access to objects based upon the identity and need to know of the user, process, and/or groups to which they belong.
File Security	The means by which access to computer files is limited to authorised users only.
Firewall	A device and/or software that prevents unauthorised and improper transit of access and information from one network to another.
Ftp	File transfer protocol. Protocol that allows files to be transferred using TCP/IP.
Hub	Network device for repeating network packets of information around the network.
Identification	The process that enables recognition of an entity by a system, generally by the use of unique machine readable user names.
Internet	World wide information service, consisting of computers around the globe linked together by telephone cables.
LAN Analyzer	Device for monitoring and analysing network traffic. Typically used to monitor network traffic levels. Sophisticated analysers can decode network packets to see what information has been sent.
Laptop	Small portable computer.
Mandatory Access Control	A means of restricting access to objects based upon the sensitivity of the information contained in the objects and the formal authorisation of subjects to access information of such sensitivity.
Modem	Device which allows a computer to send data down the telephone network.
Password	A protected, private character string used to authenticate an identity.
PBX	Private branch exchange - small telephone exchange used internally within an organisation.
Rlogin	Remote login. Protocol that allows a remote host to login to a UNIX host without using a password.

Shareware	Software for which there is no charge, but a registration fee is payable if the user decides to use the software. Often downloaded from the Internet or available from PC magazines. Normally not that very well written and often adversely effects other software.
Telnet	Protocol that allows a device to login in to a UNIX host using a terminal session.
UPS	Uninteruptable power supply. Device containing batteries that protects electrical equipment from surges in the mains power and acts as a temporary source of power in the event of a mains failure.
Username	A unique symbol or character string that is used by a system to identify a specific user.
Virus	Computer software that replicates itself and often corrupts computer programs and data.
Voice Mail	Facility which allows callers to leave voice messages for who are not able to answer their phone. The voice messages can be played back at a later tie.

BUSINESS CONTINUITY PLAN

AIM

The aim of this plan is to provide a reference tool for the actions required during or immediately following an emergency or incident that threatens to disrupt normal business activities.

An emergency is an actual or impending situation that may cause injury, loss of life, destruction of property, or cause the interference, loss or disruption of an organisation's normal business operations to such an extent it poses a threat.

An incident is any event that may be, or may lead to, a business interruption, disruption, loss and/or crisis.

The plan will help to ensure the continuation of business critical services by minimising the impact of any damage to staff, premises, equipment or records.

The plan will help to include an adequate level of detail used to maintain the business and:

- To ensure a prepared approach to an emergency/incident.
- To facilitate an organised and co-ordinated response to an emergency/incident.
- To provide an agreed framework within which people can work in a concerted manner to solve problems caused by an emergency/incident.

The plan will also help to identify actions that could be taken in advance of an emergency or incident to reduce the risk of it happening.

BUSINESS CRITICAL PROCESSES

Whilst most parts of any business are considered important, if an incident did occur, priority must be given to the restoration of the processes that are deemed to be business critical to the performance of the company.

Business critical processes can be defined as:
"critical operational or support activities without which the business would rapidly be unable to achieve its objectives"

These individual processes must be given preferential access to premises, staff, equipment or records if an emergency situation restricted their overall availability. It is for these processes that plans need to be prepared.

SCOPE OF THE PLAN

The plan will illustrate how the business can reduce the potential impact of an incident by being prepared to maintain services in the event of the:

- Loss of key premises
- Loss of key staff

- Loss of IT / data
- Loss of telecommunications
- Loss of hard data / paper records
- Loss of utilities (electricity, water, gas)
- Loss of a key partner or supplier
- Disruption due to industrial action
- Disruption due to severe weather

ASSUMPTIONS

Generally used assumptions

- The business continuity plan will cover three scenarios: for the first 24 hours following an incident and for both 2 - 7 days and 8 – 14 days following an incident. (Recovery plans needed to cover longer periods would normally be developed during the first fourteen days of an incident.)

- The business continuity plan will be reviewed regularly, with a full update on an annual basis or where a significant change to the business occurs.

Detailed Planning Assumptions

The following assumptions have been taken into account when developing the plan:

- In the event of a major incident existing business premises would be out of use for more than 7 days.

- In the event of a less significant disruption some of the existing premises would remain in use.

- Where a generator is not available loss of electricity supply across a region could last for up to 3 days.

- The mains water supplies and sewerage services may be interrupted for up to 3 days.

- Availability of the IT network historically runs at over %. In the event of a partial failure of a server the network could be unavailable for up to hours.

- If the server suite were to be completely lost it could take up to days to restore a limited desktop service (Microsoft package, E-mail and Internet access). Other software could take even longer to restore.

- Availability of the internal telephone network historically runs at %. In the event of a failure of the iSDX there could be loss of service for up to hours.

- Access to the public telephone network and mobile communications could be lost for up to 3 days.

- In a pandemic 25% - 30% of staff could be off work at any one time. This will include those who are sick, those caring for others and the 'worried well' who are simply too scared

to come to work. On average people will be absent for 5-8 days, but some may never return.

- In a fuel crisis only staff involved with delivering critical services are likely to have priority access to fuel.

THE PLAN

- Form A – Immediate Actions Checklist is a list of the actions that should be taken in response to the initial incident. The checklist is not prescriptive, exclusive or prioritised; any incident will require a dynamic assessment of issues and actions required. Depending on the scale of the incident actions can be delegated to a support team but the Senior Manager is responsible for the actions taken.

- Form B – Response Actions Checklist is a list of the actions that should be taken for the company to maintain business critical processes. The checklist is not prescriptive, exclusive or prioritised; any incident will require a dynamic assessment of issues and actions required. Depending on the scale of the incident actions can be delegated to a support team but the Senior Manager is responsible for the actions taken.

- Form C – Essential Services is a list of the essential functions undertaken by the business that must be maintained or quickly restored in the event of a disruptive incident.

- Form D – Summary of Post Incident Resources & Equipment summarises the accommodation and equipment needed to maintain operations.

- Form E – Summary of Essential IT Systems & Records summarises the basic desktop, software and systems data that need to be restored.

- Form F – Staff Details lists all service staff, indicating those business critical staff that will be required to maintain services in the event of an incident.

- Form G – Key Contacts a list of those people that would need to be contacted in the event of an incident. This could be business partners or suppliers.

- Form H – Plan Summary provides a single sheet summary of the main business continuity options of the plan.

Form A – Immediate Action Checklist

To be completed by the Senior Employee at the incident site

Action	Notes	Tick Done
If necessary: • Follow Evacuation Procedures • Call emergency services	. .	. .

Maintain a record of all emergency actions taken. Use the log in the Annex 6.4		
Assess the situation and level of response required. Can it be dealt with as a day-to-day management issue or does the business continuity plan need to be invoked?		
Communications: • Advise staff of the immediate implications for them and service provision • Advise staff of the immediate requirements to deal with situation, including temporary accommodation etc if required. • If necessary, advise key partners / suppliers. • If necessary speak to the local press.	. . . .	. . . .
If necessary, allow all staff to contact home to advise they are safe?		
If necessary arrange for the premises to be secured?		
If necessary, use signage to advise the move to a temporary location.		

Name of attending Senior Employee……..

Form B – Response Actions Checklist

To be completed by the Senior Employee at the incident site

Action	Notes	Tick Done
Once you are in control of the initial emergency update staff on a regular basis and keep them fully informed of developments. Make sure members of staff not directly involved in the incident, or those who are absent are also kept advised of developments. Refer to Form F or other staff listings.		

If necessary form a team of people to assist with the tasks required to restore services. These people should ideally be identified and trained prior to the incident.		
Priority should be given to the needs of the business critical processes.		

Advise all staff and key contacts (see Form G) of temporary location & any temporary telephone numbers to be used until numbers can be diverted.		
If mobile phones are being used make sure there are sufficient chargers available.		
Temporary Accommodation • Is the available accommodation sufficient for the needs of all the business critical processes or is additional alternative space required? • Do you need to arrange for replacement equipment to be ordered? • Do you have access to all essential systems or records? • Make arrangements for telephones and post to be re-directed to your new location.	. . . .	. . . .
Working at home and Non-Business Critical Staff • If available space is at a premium consider allowing suitable individuals to work from home • Non-essential staff should be sent home or reallocated to support business critical processes. • Make sure those sent home are aware of when to make contact to check on progress or when to return to work.	. . .	. . .
Create any new operational procedures and instructions.		
Give careful consideration to staffing levels. In a low staff level situation a priority will be a rota of replacements to avoid fatigue.		
Closely monitor staff issues, morale, overtime, welfare, etc. Do any of the staff need counselling?		

Do you need to complete an Accident Log?		
When ready, inform other organisations, public, suppliers, etc of resumption of normal service / contact details.		

Financial Procedures • Decide who can authorise additional expenditure • Keep records of all expenditure	. .	. .
Cancel or delegate any unnecessary meetings not connected to the incident		
Preservation of records • Do not destroy anything. Try to recover as many documents as possible and preserve them somewhere where they can be retrieved easily. This is an ongoing obligation throughout and after the incident. • Make someone responsible for co-ordinating and preserving a Master Log. • Make a record of all meetings and briefing sessions. • Make a hard copy of any relevant computer data and electronic mail.	. . . .	. . . .
Support the post-incident evaluation by direct contribution and by facilitating the involvement of key members of staff. Recovery should always be treated as an opportunity to improve the business.		
At the end of the recovery phase when normality is achieved, inform all interested parties and mark with an occasion.		
Review the Business Continuity Plan to learn from the decisions taken.		

Name of attending Senior Employee……

What are the essential parts of the business that are required within the first 24 hours?

What are the essential parts of the business that are required within 2 – 7 days?

What are the essential parts of the business that are required within 8 – 14 days?

Which external suppliers / partners / contractors (if any) are dependent on the services provided by your business?

Which external suppliers / partners / contractors (if any) does your business depend upon?

Form D – Summary of Post Incident Resources & Equipment

(Excluding IT as these should be given on Form E)

Requirement	Within 24 hrs	2 – 7 Days	8 – 14 Days
People			
Number of staff (FTE)			
Furniture			
Chairs			
Desks			
Filing cabinets			
Equipment			

Office Phones			
Mobile Phones			
Desktop PC			
Laptop PC			
Printers			
Fax			
Scanner			
Photocopier			
Records			
Paper records/files			
Special Provisions			

Confidential area			
Secure area for safe			
Delivery area / Mailroom			
Air conditioning			
Storage space			
Waiting Room			
Public Access			
Wheelchair Access			

Form E – Essential IT Systems & Records

Requirement	Within 24 hrs	2 – 7 Days	8 – 14 Days
Desktop			
Microsoft Office			

E-mail			
Internet Access			
Additional Software			

Essential Computer data			

Form F – Staff Details

If an alternative list exists add details about who has access and where both paper and electronic versions are held. This avoids having to keep more than one listing updated.

NAME	POSITION/ROLE	KEY	ADDRESS	HOME	MOBILE

Form G – Key Contacts

If an alternative list exists add details about who has access and where both paper and electronic versions are held. This avoids having to keep more than one listing updated.

NAME	POSITION/ROLE	E-MAIL ADDRESS & OR BUSINESS PHONE	HOME	MOBILE

Form H – Plan Summary

Identified Risk	Recovery Option	Evaluation Criteria	Possible Further Action
Loss of Accommodation			
Loss of Staff			
Loss of IT / Data			
Loss of Telecommunications			
Loss of Hard Data / Paper Records			

Loss of Mains Services (Electricity, Water and Gas)			
Identified Risk	Recovery Option	Evaluation Criteria	Possible Further Action
Loss of a Key Partner / Supplier			
Disruption due to industrial action e.g. fuel shortage			
Severe Weather			

ANNEX

Assessing the risks

Use this table to produce an assessment of the current risks to your business and/or location.

Likelihood	Impact
Low	Low
Medium	Medium
High	High

Risk	Likelihood	Impact	General Control Measures	Possible Further Action
Fire completely destroying all of part of the premises				
Theft of computer or office equipment				
Loss of staff (Pandemic)				
Loss of staff (Serious incident / accident)				

Loss or corruption of IT data				
Loss of telecommunications				

Risk	Likelihood	Impact	General Control Measures	Possible Further Action
Loss of Electricity				
Loss of Water				
Loss of Gas				
Flooding				
Storm Damage				
Fuel Shortage				

Vandalism				
Terrorist threat				
External factor preventing access to premises e.g. fire, police incident, traffic accident				
Loss of a key partner or supplier				
Risk	Likelihood	Impact	General Control Measures	Possible Further Action
Disruption due to industrial action				
Disruption to the transport network				

JULICA CA

Business Continuity and Disaster Recovery Plan

Company Mobile Phone Users

Laptop users

Staff able to work from home

Emergency Operations Log

Incident:	Date:	Sheet ….. of …..

Time	Event	Action

TRAINING & REVIEW DATES

The plan will next be tested in

The plan will next be reviewed in or earlier in the event of a significant change to the business.

JULICA CA
Business Continuity and Disaster Recovery Plan

Introduction

The Senior Management of JULICA CA (hereinafter referred to as the Organization) recognize the need to protect employees during an emergency and to have detailed recovery plans to provide for the continuity of operations of the

Organization in an emergency or disaster situation. This document has been developed to meet those needs and it will be used in the event of a disaster or emergency.

This Plan could be implemented as a result of many types of disasters, including natural disasters such as flood, fire or severe weather, technical disasters, such as equipment or power failures or human events, such as terrorism or vandalism. Since the number and type of emergencies that could occur is quite numerous, the Plan is written to cover a major emergency or disaster and the Plan will be adapted to the situation or disaster faced.

Purpose and Scope

It is the intention of senior management to continue service to its customers in spite of any unplanned and extended interruption of primary business functions. The purpose of this document is to designate who will be responsible for making critical decisions during an emergency situation and to provide guidelines to be followed in an emergency. Plan assumptions are defined below.

- The Plan seeks to minimize the financial exposure and vulnerability of the Organization.
- The level of recovery for any specific function is determined by the critical nature of the various business functions as well as the need to maintain public confidence and credibility.
- The Plan will be amended as changes in the business environment occur.
- The Plan will be reviewed my management, internal and external auditors and regulatory examiners as requested.

Plan Objectives

The major objectives of this Plan are listed below.

1. Protection of personnel
2. Protection of property and records
3. Continuity of management
4. Restoration of critical function within 24 – 48 hours
5. Restoration of essential functions within 72 hours
6. Eventual resumption of normal operations including all non-essential functions

Management Succession

In an emergency situation following a major calamity, procedures may be needed to ensure that the

Organization's remaining officers have the authority to direct immediate recovery operations to speed the resumption of vital operations. The following specific measures are to be implemented to maintain continuity of leadership.

Executive Succession

In the event of an emergency, the officers and employees of the Organization will continue to conduct the affairs of the Organization under such guidance from the senior management as may be available subject to conformance with any governmental directives during the emergency.

Senior management shall have the power, in the absence or disability of any officer, or upon refusal of any officer to act, to delegate and prescribe such officer's powers and duties to any other officer or director.

If the Chief Executive Officer cannot be located or is unable to assume or continue normal executive duties, then the authority and duties of the CEO shall, without further action of senior management, be automatically assumed by one of the following persons in the order designated.

- Managing Director
- Consulting Services Director
- Director of Operations and Technology Services
- Chief Financial Officer

In any emergency, all officers and employees should proceed to the Organization or to the relocation site as appropriate. As soon as possible, the person whose name appears highest on the succession list will become the Organization's acting Chief Executive Officer until the arrival of someone higher on the succession list. At all times, the available person whose name is highest on the succession list will be the Organization's acting Chief Executive Officer.

Administrative and Other Personnel Succession

The administrative and personnel succession shall follow a similar plan where succession for each department will flow from the Department Manager to the next highest level employee in the department in the event the Department Manager is unable to assume or continue normal duties.

Emergency Team Assignments and Responsibilities

Emergency Response Management Team (ERMT)

Senior Management of the Organization has delegated the responsibility and authority for the institution, operation, monitoring and revision of the Plan to the Emergency RespoSenior Management is committed to providing the Team sufficient support and resources to carry out the responsibilities and duties set forth in this Plan.

The Team is also responsible to assess the nature of damage sustained in the event of a disaster

situation and to implement the Plan. Each member of the Team will maintain a copy of the Plan to ensure easy and quick access in the event of a disaster situation.

In addition, each member will be responsible for informing the other members of the Team regarding any plans for extended absences (three days or more) from the immediate area. If an extended absence is anticipated, members must be informed of the absent member's itinerary.

The basic responsibilities of the Team are as follows.

1. Develop, oversee and monitor the Organization's Plan.
2. Define the critical and essential functions of the Organization and determine in what order the functions will be restored.
3. Analyze the Organization's exposure to the various types of threats and vulnerabilities and establish emergency procedures to follow.
4. Establish a chain of command for notifying people in the event of a disaster.
5. Develop communication procedures to adequately inform and direct all levels of management and other personnel during emergency situations.
6. Develop procedures to take care of customers during an emergency.
7. Evaluate the adequacy of critical technology service providers' contingency plans.
8. Ensure that backup sites are supplied with appropriate materials.
9. Authorize special assignments as needed.
10. Approve expenditures relating to the Plan.
11. Evaluate the Organization's insurance coverage to ensure that it is up-to-date and adequate for current needs.
12. Adequately train personnel in disaster preparedness and evacuation procedures.
13. Ensure that the Plan is tested at least annually.
14. Meet at least annually to review and update the Plan.
15. Periodically report findings/recommendations to the Board for its review.

ERMT Areas of Responsibility

The first person to recognize the disaster will contact the appropriate Emergency Agency Contact List)and the Team Leader and other Team members. Once notified, Team members will gather at the location of the disaster or alternate location if necessary and will begin to carry out responsibilities defined below.

Emergency Coordinator – CHRIS DANIEL

- Manage and direct the recovery effort, coordinate teams, monitor recovery schedule, and serve as contact person for recovery services.

- Coordinate financial resources necessary to respond to the disaster and authorize expenditures.
- Works with Public Relations for all media communication.

In addition to the broad responsibilities of the designated Team leaders, individual Team members will carry out responsibilities defined below according to their area of assignment. Each Team member may appoint individuals to serve as members of a specific recovery team as needed. If a recovery area leader appoints a team, he or she is responsible for notifying the ERMT of the employees that make up the appointed team.

Damage Assessment

- Evaluate the initial status of the damaged area and estimates both the time to reoccupy the facility and the salvage value of the remaining equipment.
- Oversee the salvage of equipment and data; identifying which resources remains.

- Determine the future utilization of salvaged items in rebuilding and recovery from the disaster.
- Coordinate clean up at the disaster site.

Safety

- Ensure that first aid is available at the emergency site. Ensure that all employees are accounted for.
- Notify employees' families of emergency situation.
- Handle all personnel and injury issues.

Security

- Protect the assets and records of the Organization by oLocking all doors as needed

oGathering all purses and valuable items that may have been left behind oDistributing valuables to owners or placing in a secure location Contact security guard if needed.

Communications

- Initiate calling tree for contacting employees (Notify the insurance company. Notify regulatory authorities.

Facilities and Supplies

- Coordinate with vendors on the replacement of equipment and suppliesOffsite Storage and Disaster Supplies). Locate a temporary working facility, if necessary.

Information Technology Recovery

- Implement all detailed recovery procedures for information technology functions.

Information Technology Recovery Team

Members of the ERMT have been assigned responsibilities for specific areas. In addition to the ERMT, an Information Technology RecoveryTeam has also been established to deal specifically with recovery of technology systems and operations of the Organization. This Team shall be directly responsible for the actual restoration of business functions by implementing defined recovery procedures of the Plan.

Functional Area Response Members (FARM)

These individuals have the basic responsibilities defined below.

1. Establish detailed recovery procedures to be followed in an emergency or disaster situation.
2. Assure that their remote locations are implementing departmental or remote location backup procedures and storing backup media properly.
3. Restore communications within their respective remote location.
4. Assure that there is ongoing training for new personnel.
5. Account for each employee in their area in the event of an emergency.

FARM members will coordinate with ERMT to assure that procedures have been established for the remote location to be able to function after an emergency or disaster.

Under the overall direction of the Emergency Response Management Team, support is provided to assist an area's recovery by Functional Area Response Members. These teams work in conjunction with the Emergency Response Management Team. They work to restore services and provide assistance at the operation level to the area affected by the problem condition and to restore services.

Risk Assessment and Business Impact Analysis

In addressing contingency planning, Senior Management is aware of the potential risks that may arise. Disruption to operations can impact the Organization for both the short term and long term. There are various types of risks and many scenarios that could put the Organization at risk. A detailed analysis follows defining the risk areas and an analysis of possible scenarios with probabilities and impact levels assigned.

Types of Risk

Appropriate planning is done to minimize the following risks. Any combination of these risks is present when an emergency occurs, disrupting normal operations of the Organization.

Compliance risk

In an emergency, it is important for the Organization to maintain legal compliance with various appropriate regulations as well as compliance with the organization's data processing emergency and disaster recovery preparedness policies. The Plan will take into account compliance and regulatory issues in the development of all recovery procedures.

Transaction or operational risk

Transaction or operational risk can impact earnings or capital due to problems with service or product delivery resulting from an emergency situation. Transaction or operational risk occurs in the delivery of all products and services, and it may be addressed through consideration of all aspects, including data input, data processing, data output, Internet based services, and network services. People, equipment, systems, data files, and other significant elements of the Organization's processing ensure the restoration of processing and service within a short timeframe and are critical to customers of the organization and the viability of the Organization.

Strategic risk

Strategic risk management involves addressing the potential adverse business impact to the organization, both internally and externally, that may occur if the Organization is unable to restore network, data processing operations, and related functions within an acceptable time frame. If the strategic risks related to data processing disaster recovery are not understood, addressed, and managed in terms of preparedness, the Organization may not be able to address the risks and related solutions in the short term, resulting in economic and market losses.

Reputation risk

Developing and retaining marketplace confidence in handling customers' transactions in an appropriate manner, within an acceptable time frame, as well as meeting the emerging needs of the customer base and community, for example, after a disaster, are important in protecting the safety and soundness of the Organization.

Scenarios and Probability

The Organization faces a number of emergency situations that could interrupt business. The Organization could experience an interruption as a result of natural causes, unnatural causes or technological causes as summarized below.

Scenario	Probability	Potential Impact
Natural Causes		
Fire	Medium	High
Flood	Low	High
Hurricane	Very Low	High
Tornado	Medium	High
Earthquake	Very Low	Medium
Other severe weather	High	Low
Air contaminants or hazardous spills	Low	Low
Human Threats & Malicious Activity		
Civil strife	Very Low	Low
Virus	Medium	Medium to High
Network security attack	Medium	Medium
Fraud, theft or blackmail	Low	Medium
Arson	Low	High
Vandalism	Low	Medium
Terrorism	Very Low	High
Bombing	Very Low	High

Technical Threats		
Hardware or software failure	High	High
Communications failure	Medium	High
Power failure	High	Medium

. Emergency procedures for the high-rated natural causes, human threats and malicious activity are included in the Emergency Procedures section of the Plan. Procedures for recovery of complete business functions are included in the Functional Area Recovery Procedures section of the Plan. Procedures for recovery from all technical threats are detailed in the Information Technology Recovery Procedures of the Plan. Procedures for recovery of remote location locations are included in the Remote Location Recovery Procedures section of the Plan.

Some scenarios that are not rated to have a high impact or high probability may actually result in the need to follow either emergency procedures, such as a building evacuation, or recovery procedures, such as restoring an electronic system. Defined procedures for high probability/impact scenarios will be followed as appropriate should another scenario not specifically addressed occur.

Assessment of Functions

Every Organization function and department has been considered and evaluated as to the downtime allowable and recovery time objectives. Functions have been categorized according to the disruption that would be caused if the function were not available and have been classified using the following categories.

Critical - the loss of the function would seriously jeopardize operations after one day disruption of service

Essential - the loss of the function would seriously jeopardize operations after a one week disruption of service

Non-Essential- the performance of the function is convenient and necessary to customers and the Organization but the lack of such function does not seriously detract from operating capabilities

Critical Functions

The following areas have been identified as those critical to the overall operation of the institution and contingency or recovery plans must be maintained for these areas.

- Core business processing – Communications via Cell, Land Line or E-mail
- Data Center (or server room) – What systems are in your DC (including WAN connectivity)
- Human Resources – Payroll
- Internet Services including External Website

Essential Functions

The following areas have been identified as those essential to the operation of the institution and recovery plans may be maintained for these areas.

- Remote Location Communications (Phones & External Telecommunications)
- Primary Email (Use alternative if available)
- Operations, Administration and Accounting - Accounts Payable
- Network – User data folders and other applications (SharePoint)
- Printing
- Facilities

Non Essential Functions

- Company Operations, Other accounting functions not listed above, Regulatory Reporting
- Investments and Asset Liability Management
- Human Resources - All functions other than payroll
- Demo and Test Virtual Machines
- Customer Access to Virtual Services – White Papers and Tutorials

Recovery Priorities

Efforts will be devoted restoring Critical functions first. Once Critical functions have been restored, efforts will be devoted to re-establishing Essential functions. After all Critical and Essential functions have been restored, attention will be given to restoring Non-Essential functions and services.

Critical functions will be restored for the most part in the order the functions have been listed however recovery efforts will more than likely be simultaneous for all Critical functions.

Classification of Disasters

The impact of a disaster will be assessed by the ERMT and classified as follows.

- Level 1 - No interruption in operations.
- Level 2 - Some facility and computer equipment damages observed, but operations can be resumed within 8 hours.
- Level 3 - Moderate damage to the facility and/or the computer equipment is observed, but operations can be resumed within 8 to 48 hours.
- Level 4 - Major facility and computer equipment damage is observed with interruption in operations for over 48 hours. All personnel and functions must be moved to the Designated Alternate Site.

Recovery procedures have been developed considering the seriousness of a disaster and the levels described above. Most functions have recovery procedures that will be used in all Level 1, 2 or 3 disasters and then additional procedures to be used for a Level 4 disaster. For example, manual processing will be used for most emergencies lasting up to 48 hours (Levels 1, 2 and 3) before processing is actually moved to the offsite location due to a Level 4 disaster.

Declaring a Disaster

Once an emergency or disaster has occurred, the Alternate Emergency Coordinator, the ERMT member assigned with Damage Assessment responsibility, will assess the damage in order to determine the level of the disaster. A disaster will be declared only if the damage is determined to be major, sufficiently warranting a Level 4 status. The ERMT Team Leader, Emergency Coordinator and Alternate Emergency Coordinator will meet after the initial damage assessment to collaborate on such a decision. At that point a disaster will be declared, emergency and recovery procedures will be implemented, and Organization functions will move to the alternate location defined below. Two of these individuals (Team Leader, Emergency Coordinator or Alternate Emergency Coordinator) may also declare a disaster if all three are not available to discuss the situation.

Alternate Locations

If main office is temporarily or permanently unable to continue operations, the first location listed below will become the acting head office of the Organization. If the first location is not available, the second location listed will become the acting head office of the Organization.

- Primary Office: (Location)
- Secondary Office: (Location)

Records Protection

The Organization has implemented a number of systems and procedures to protect the records of the Organization. Both electronic and paper records must be protected. The Organization should be able to reconstruct its position and account relationship with customers following an emergency. To achieve this, the Organization archives various records in locations not in the immediate area of the Organization. A copy of all data files and software is retained along with photocopies, microfilm or optical disks containing other Organization records, such as notes and collateral.

Insurance

The Senior Management must review the insurance coverage for the Organization on an annual basis. The Organization believes that it has sufficient insurance coverage to guard against loss from risks that cannot be completely prevented. In reaching this conclusion, the Organization assessed the possible hazards and the potential dollars at risk versus the costs of insuring.

In the event of a disaster that requires insurance claims to be submitted, such claims are to be filed immediately. All proceeds from the payment of the insurance claims will be utilized to replace or restore damaged structures and equipment at the first possible occasion. A list of the Organization's insurance carriers and the coverage provided.

Employee Training

Testing of the Plan is an essential element of preparedness. All Organization employees will be trained in emergency procedures annually. In addition, employees

that have roles defined in the Plan will be trained to carry out their individual responsibilities defined in the Plan.

Plan Testing

The Plan will be tested annually. A summary of the testing results will be presented to Senior Management. Testing will include, at a minimum, the following areas.

- IT Recovery procedures for all critical applications
- Emergency procedure testing
- Remote location emergency and recovery testing

Plan Maintenance

The Plan will be reviewed annually to determine if revisions are needed. New services, changes in location, and changes in vendors will be considered during the review. Changes will be made and the revised Plan along with a summary of all Plan testing will be presented to Senior Management. Each time revisions are made, updated copies will be distributed to all Team members and an updated copy will be taken offsite.

Emergency Procedures

General Overview

Upon information being received of any of the following natural disasters, the ERMT working with the Emergency Coordinator will review the situation and declare the recommended plan for the situation. If the timeline of the disaster is sufficient to allow staff to return safely to their homes, employees may be asked to continue working until close of business, which allows for time to make last minute preparation before shutdown of the institution. However, if an immediate situation arises, the Emergency Coordinator will declare specific actions.

Emergency Evacuation Procedures

There may be instances because of fire, bomb threats, etc. when it will be necessary to evacuate the building as rapidly as possible. When an employee becomes aware of an emergency, he/she must immediately notify his/her supervisor or a senior member of staff at the branch location if his/her supervisor is not at that location. That person in turn will notify Senior Management and Civil Authorities.
Managers are responsible for supervising the evacuation of their respective areas. Personnel are reminded that personal safety is of first and foremost importance in these emergency evacuation procedures. Steps that cannot be safely completed should be ignored.

1. Escort all customers out of the office immediately. Office exits will then be secured and no one shall be permitted to enter the office. Secure doors when notified by the Senior Officer to do so.

2. All employees should secure their work area and then proceed through the front door. If the front door is not accessible, then, you should proceed through an alternate exit if available.

3. Supervisors should attempt to secure all valuable records in a cabinet or locked desk.

4. Employees should shut down or lock workstations before exiting the building if time permits.

5. The IT Department should follow the Emergency Shut Down Procedures described in the next section.

6. All staff should proceed with customers to disaster-designated meeting places outside the building. Each branch office has a different meeting location outside the building, please see your local office emergency procedures.

7. DO NOT USE ELEVATORS. Evacuate the premises using the stairwells.

8. Do a quick visual inventory before leaving to see if any staff or customers are still on site. DO NOT TRY TO RESCUE THEM, proceed outside and immediately advise a member of Management of anyone left inside. It is important to be specific if someone is missing, providing the location and last time that person was sighted. If the person's name is known or some description is possible, please try to remember as you leave the premises. Department Heads must verify that all personnel are accounted for.

9. Do not reenter the building until instructed to do so.

If the building is not vacated, staff should remain calm and stay within their work areas until further instruction is provided. The ERMT should immediately proceed to a conference room to discuss the disaster, implement the plan, and initiate individually assigned responsibilities.

If after hours, the individual contacted will initiate the calling tree to ensure that all members have been notified. Depending on the type of disaster, the ERMT will either proceed to the Organization to assess damage or initially meet at a designated nearby location.

Emergency Shut Down Procedures

The following procedures are to be followed in an emergency. A copy of these procedures is posted on the door the computer room and all IT personnel have been instructed to follow these procedures.

Recovery and Restart Procedures

The following procedures are to be followed after an emergency to restore systems. A copy of these procedures is posted on the door to the computer room and all IT personnel have been instructed to follow these procedures.

Medical Emergencies

During a medical emergency, employees should use the following guidelines.

1. **Remain Calm** and immediately call for rescue squad or ambulance.

2. To insure adequate breathing, open and maintain the victim's airway by gently

tilting head back. If victim is NOT breathing, immediately begin mouth-to-mouth resuscitation.

3. Check and periodically recheck the victim's carotid pulse in the neck, using two fingers. If pulse is not present, immediately begin CPR.

4. Stop all obvious bleeding by applying direct pressure over the wound with your hand. If available, use a clean cloth or bandage.

5. Do not move victim unless a hazard is present. Keep the victim in a quiet, comfortable position.

6. Loosen all tight clothing.

7. Keep victim warm - do not induce sweating.

8. Give no fluids - except very small sips of water, only if requested by the victim.

9. Elevate victim's legs slightly, unless an injury is present on the chest or head.

10. Comfort and reassure the victim constantly.

11. For all on-the-job injuries, notify your supervisor as soon as possible.

Loss of Electrical Power

A loss of electrical power can prove to be a serious situation for all institutions. Not only does it pose a security threat and loss of communication, but also physical threat with the loss of air or heat.

As soon as a power failure has occurred, a member of the ERMT will contact or designate an employee to contact the power company to report the outage and determine if there is an expected time for restoration of power. Based upon the information obtained, a decision will be made as to the next steps to be taken.

In cases of extended loss of power, the ERMT may declare an emergency and the premises vacated. If the building is to be vacated, employees should follow the basic emergency evacuation procedures described above. A sign stating that the Organization has been closed will be posted. The local police will be contacted to alert them of the power failure and the evacuation of the building. The remaining remote locations also will be notified regarding the status of the outage for customer inquiries.

Systems that are on UPS battery backup should be monitored. If the outage is over 30 minutes, plans should be made to shut down servers according to the procedures described above.

Fire

In the event of a fire that IS NOT AN IMMEDIATE DANGER, the following steps should be taken:

1. Notify Management immediately.

2. Set off the nearest fire alarm to alert others.

3. If the fire has not advanced too far, attempt to control it with a fire extinguisher.

4. If the fire is in the computer room and the IT manager is not present at the time of the emergency, immediately notify him if possible.

5. If the fire is located in the computer room and equipment is not in immediate danger and accessible. Shut down equipment according to the procedure listed above.

6. Exit the building, closing doors and windows behind you when leaving your work area.

7. When exiting the facility, check all closed doors for extreme heat before opening any doors. Lightly touch the door to feel for extreme heat. If the door is not extremely hot, cautiously open the door, and when deemed safe, enter the corridor and close the door behind

you. If the door is extremely hot, DO NOT OPEN THE DOOR, but retreat as far away from the door and adjoining wall as possible and signal for help from a window.

8. Notify the fire department.

If the fire is determined to be an immediate threat to personal safety, personnel are instructed to implement the evacuation procedures in this policy, closing all doors to the fire area, and notifying the fire department when they are safely away from the area.

Flood or Water Leakage

The following procedures should be followed in the event of a flood or water leakage.

1. Notify Management immediately.

2. Shut down all electrical equipment, by turning off the appropriate circuit breakers after a normal shutdown. The degree of 'normal' shutdown will depend upon judgment and under no circumstances should an employee be subjected to any greater danger than necessary.

3. Cover equipment with protective plastic sheets, if available.

4. Move all data stored on removable media to a safe place.

5. Move critical workstations and servers to a safe place if time permits. At a minimum, any workstations located on the floor should be moved from the floor to the desk.

6. Depending upon the severity and location of the flood, a member of the EMRT, the Department Head or Remote Location Manager will contact the appropriate persons to stop water entry if possible and/or to remove water.

7. Judgment is to be used to determine the severity of the situation, which will dictate further actions to be taken.

Natural Phenomena

In case of a natural disaster such as a hurricane or flood, the Organization will allow employees to return home within a reasonable time to secure themselves and their families. Employees are to make every effort as soon as possible to notify Management of the Organization if he/she is a victim of such a disaster.

Tornado Procedures

Employees of the Organization are to move to the center of the floor on which they work away from windows and glass if they are alerted of an impending tornado. Shelter should be taken in rooms without windows if possible at the most interior portion of the building.

Terrorism or Bomb Threat

If an employee suspects that a bombing device is present, extreme caution must be exercised and the following steps should be considered.

1. Notify Management to immediately call 911.

2. The Department Supervisor should contact the most senior member of the ERMT.

3. Determine the answer the following questions:
    a. Is this an isolated circumstance?
    b. Is the threat specific?
    c. Is time imminent?
    d. Is the threat plausible?
    e. Is the caller convincing?
    f. Is the danger avoidable?

4. The ERMT is responsible for inspecting the premises to locate unidentifiable or unexplained objects or packages only under the direction of emergency workers. Consider such items as briefcases, luggage, shopping bags, purses, and wrapped packages. Be as thorough as possible, time permitting. In general, any place with public access such as restrooms, conference rooms, and unlocked storage rooms, public lobbies, trashcans, elevators, or stairwells, etc. should be inspected.

5. Use extreme CAUTION and do not touch or attempt to move a suspicious object.

6. Take appropriate action to protect employee and customer property.

7. Explain the situation to other employees in an effort to avoid panic and prepare for orderly response.

8. Evaluate the possibility of evacuating.

Summary of Basic Disaster Plans

The Organization has an agreement with Africa Data Center for backup processing. In the event of a disaster, the Organization's basic plan is to operate in a mostly manual environment for up to two days. If recovery cannot be expected within two days, processing will likely be moved to the offsite recovery center.

Functional Area Recovery Procedures Emergency Teams

The Emergency Response Management Team (ERMT) shall be composed of the following individuals.

Name	Title	Position	Recovery Area of Responsibility
	President & CEO	Team Leader	Public Information
	Chief Financial Officer	Emergency Coordinator	Communications
	Personnel Manager	Team Member	Safety
	Remote Location Operations Manager	Team Member	Facilities and Supplies
		Team Member	Information Technology Recovery
	Technology Services Manager	Team Member	Information Technology Recovery

The Information Technology Recovery Team (ITRT) will be composed of the following individuals.

Name	Title	Position	Primary Responsibility
	IT Manager	IT Recovery Coordinator	Network infrastructure
	Operations Manager	Operations Recovery Coordinator	Core System
	Network Administrator	Team Member	Network servers
	Desktop Support Technician	Team Member	Workstations

JULICA CA

Business Continuity and Disaster Recovery Plan

The following individuals are Functional Area Recovery Members (FARM) of the Disaster Team.

Name	Functional Area of Responsibility
	Operations
	Accounting

Emergency Contact List

Contact	Contact Information
Local Police Department	
Local Fire Department	
Ambulance Service	
Hospital	
Telephone Company	
Gas/Heat Company	
Electric Company	
Building Manager	
Building Security	
FEMA Regional Office	
Media	
Newspaper	
Television Stations	
Radio Stations	
Insurance Agent	
Regulatory Agencies	
Hotsite Vendor	
Generator Vendor	

- Employee Contact List

Contact information for all Organization employees is documented below. Each Department and/or Remote Location Manager will be responsible for notifying all employees within their Department or Remote Location of the emergency situation.

Employee Name	Home Phone Number	Cell Number	Emergency Contact Name & Number	Alternate email address
CHRIS DANIELS	0721138882			mail@tenda.world
CHRISTINA WANJIKU	0795289184			mail@tenda.world
JAMES OSORE	0741138530			mail@tenda.world

E - Offsite Storage and Disaster Supplies

General Supplies Inventory

These general supplies are maintained at the Main Office and at each remote location

- NOAA Weather Radio
- First Aid Kit
- Flashlights/Batteries
- Waterproof Plastic Bags
- Camera/Film
- Pens/Pencils/Paper
- Small supply of water & nonperishable food
- Tool kit (basic tools, gloves, etc.)

Key Operations Vendors

In addition to the general supplies listed above, the following items are also maintained in *<insert location here>.* Detail supplies for each Remote Location and Department are listed within the Remote Location and Functional Area Recovery Procedures.

<This is a sample list. This list is compiled after each functional area and remote location determines the supplies needed. The supplies for each functional area or remote location do not need to be listed individually here. The forms or supplies can be placed in a large envelope and labeled then

referenced here.>

Item	Supplier/Person Responsible
Letterhead and envelopes	
Accounting Supplies	
Data Processing Supplies	
Operations Supplies	
Add Disaster Companies	

Backup Drives and Software Inventory

The following backup drives and recovery items are retained at *<list offsite tape storage>*. These items are stored in *<a locked fireproof cabinet>* at the offsite location. *<List individuals>* are the only individuals that can access the items as the offsite location.

Backup Drives

- Daily backup tapes for core business system (two week rotation of 2 tapes for each day)
- System save backup tapes (one for each of previous 12 months)
- Network backup tapes (two week rotation, 1 DLT tape for each day) Month end network backup tapes (one for each of previous 12 months)
- Etc.

Software

- All software is able to be re-downloaded from the Internet all local copies are recoverable.

Other Recovery Items

These items that are needed for recovery are also retained offsite.

Item	Responsible Party
Copy of Business Continuity and Disaster Recovery Plan	
Organization Policies & Procedures	
Daily Processing Instructions	
Backup Procedures	
Blueprints of the Main Office	

Appendix G – Telecommunications Circuit Information

Below is a listing of the Organization's telecommunications circuits.

Circuit Description	Vendor	Circuit #	Termination Location

Functional Area Testing Summary

Functional Area	
Classification of Functions	Critical Functions Essential Functions Non Essential Functions
Emergency Procedures Specific to Functional Area	
Systems &Software Relied Upon	
General Resources Needed	

Function	
Supplies and Documents Needed	
Recovery procedures	

Function	
Supplies and Documents Needed	
Recovery procedures	

IT Recovery Testing Summary

Application or System	
Classification	
Maximum allowable downtime desired by Organization	
Anticipated recovery time	
System details	
Backup and redundancy	
Detailed recovery procedures	

Remote Location Recovery Testing Summary

Remote Location Tested	
Disaster Scenario(s)	
Summary of Actions	
Persons Involved	
Test Date	
Results	
Plan Changes Needed	
Detailed Testing Procedures	

Subscriber Agreement

This Subscriber Agreement (this "Agreement"), is entered on the "Effective Date", between Tendaworld Ltd., a limited company formed under the laws of The Republic Of Kenya, with registered number PVT-AJU3G6G and registered offices at P.O. Box 386, 00517 2nd Floor, ICEA Lion Centre, Riverside Park Nairobi, Kenya, ("Tendaworld") and The Subscriber.

Whereas, Tendaworld provides electronic certification, software-as-a-service, hosting, products, and/or other services to its customers. Subscriber now wishes to include Tendaworld's Subscription Services and plarform services as part of Subscriber's product offering.

The parties therefore agree as follows:

1. Entire Agreement. This Agreement consists of the following documents:

   (i) this signature page,

   (ii) the General Terms and Conditions listed here:Tendaworld-General-Terms-and-Conditions-v2.1.pdf, which is incorporated herein by this reference, and (iii) the Schedules attached hereto.

   The General Terms and Conditions, this signature page, and the Schedules attached hereto constitute the complete agreement between Subscriber and Tendaworld and supersede any prior discussions, representations, or click-through agreements executed between the parties. Nothing contained in any purchase order, purchase order acknowledgement, or similar document shall in any way modify or add any additional terms or conditions to this Agreement. Subscriber understands and agrees that any additional or conflicting terms in Subscriber's current or future purchase orders, which are not included in this Agreement are deemed rejected and are not part of this Agreement between Tendaworld and Subscriber.

2. Representations. Subscriber represents that it has read, understands and agrees to be bound by the General Terms and Conditions and Schedule(s) referenced, attached, or incorporated into this Agreement.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their duly authorized representatives effective on the Effective Date.

Subscriber

Name:

_____

Effective Date:

_____

Signature:

_____

Address for Notices:

Hiring Policy and Procedures

Objective

JULICA CA believes that hiring qualified individuals to fill positions contributes to the overall success of the company. Each employee is hired to make significant contributions to JULICA CA. In hiring the most qualified candidates for positions, the following process should be followed.

Hiring Process and Procedures

Personnel requisitions

Personnel requisitions must be completed to fill JULICA CA positions. Requisitions must be initiated by the department supervisor/manager, approved by the division vice president and then forwarded to the human resource (HR) department.

Personnel requisitions should indicate the following:

- Position title.
- Position hours/shifts.
- Exempt or nonexempt status of the position.
- Reason for the opening.
- Essential job functions and qualifications (or a current job description may be attached).
- Any special recruitment advertising instructions.

Intake meetings

HR will arrange a meeting with the hiring manager to conduct an intake meeting prior to posting a job opening to learn more about the position, the requirements and the profile of the ideal candidate. The recruiting strategy will be set during this meeting and expectations established with all the key stakeholders.

Job postings

HR will create job postings that briefly describe the job opening and communicate JULICA CA brand. All job openings will be posted concurrently on JULICA CA intranet and externally with sources appropriate for the position being filled. Jobs will remain posted until the position is filled.

The HR department will be responsible for tracking all applicants and retaining applications and resumes as required.

Internal applicants

Current employees with a satisfactory employment status may apply for internal job openings. The consents of the employee's manager and the HR department may be necessary for employees with less than one year of service with JULICA CA.

All applicants for a posted vacancy will be considered based on their qualifications and ability to perform the job successfully. Internal candidates who are not selected will be notified by the HR department.

Interview process

The HR department and the hiring manager will screen applications and resumes prior to scheduling interviews. Initial interviews are generally conducted by the HR department and the hiring manager using behavior-based interview questions and a structured interview process. Candidate evaluation forms will be completed after each interview and retained with the application.

The HR department will notify applicants who are not selected for positions at JULICA CA.

Reference checks

HR will conduct professional reference checks and employment verification on the top candidates based on the results of the candidate evaluation forms completed by the interviewers. A minimum of three professional references are required from each candidate.

Job offers

After a decision has been made to hire a candidate, an offer will be made contingent on the satisfactory completion of required background checks and testing. Background checks will vary depending on the position and may include criminal history, credit history, driving record, drug testing or any other relevant information for the job.

Internal applicants must complete required background checks or tests not previously completed.

Once the HR department receives satisfactory results from all required background checks and tests, candidates will be provided with a final job offer. If a candidate fails to accept an offer of employment within 7 calendar days, the offer may be rescinded by the company.