



Business Continuity Plan

Last updated: May 2026

Contents

BUSINESS CONTINUITY PLAN	1
Document Version	3
Plan Amendments	3
Distribution List	Error! Bookmark not defined.
References and related documents.....	3
SECTION 1 INTRODUCTION	4
1.1 Objectives	4
1.2 Glossary	5
SECTION 2 RISK MANAGEMENT PLANNING.....	6
SECTION 3 BUSINESS IMPACT ANALYSIS.....	6
3.1 Natural disaster.....	6
3.2 Pandemic.....	7
3.3 Political instability	8
3.4 Civil unrest.....	10
3.5 Cyberattack	10
3.5 Business Impact Analysis.....	12
SECTION 4 INCIDENT RESPONSE PLAN.....	14
4.1 Natural disasters	14
4.2 Pandemic.....	14
4.3 Political instability	15
4.4 Civil unrest.....	15
4.5 Cyberattack	16
4.6 Immediate Response Checklist	16
4.7 Evacuation procedures & Emergency kits.....	17
4.8 Roles and Responsibilities	17
SECTION 5 RECOVERY.....	19
5.1 Natural disasters	19
5.2 Pandemic.....	19
5.3 Political instability	20
5.4 Civil Unrest	20
5.5 Cyberattack	20
5.6 Recovery Plan.....	22
5.7 Incident Recovery Checklist	23
5.8 Recovery contacts	24
5.9 Insurance claims.....	24
SECTION 6 PREPARATION & PREVENTION.....	25
6.1 Natural disasters	25
6.2 Pandemic.....	25
6.3 Political Instability	25
6.4 Civil Unrest	26
6.5 Cyberattack	26
6.6 General preparations	26

Document Version

Date	Comments
July 2020	Business Continuity Plan drafted
October 2020	Draft updated to include cyberattacks
May 2026	Removal of Friends of Femili PNG (FPNGA); minor changes and updating

Plan Amendments

This is a working document and subject to amendment. Any suggestions about this Policy should be directed to the Femili PNG Operations Directors, IT Manager or Chief Executive Officer/Senior Social Worker (CEO/SSW) so changes can be considered. When suggestions are raised, the matter will be raised with the Executive Management Committee (EMC) for consideration. Any amendments or changes to the Policy will be submitted to the Board for endorsement.

The Operations Directors, IT Manager and CEO/SSW is responsible for maintaining this document; including updating confirmed changes, informing staff of the changes, and disseminating the latest version across the organisation.

Any changes or amendments involve the following steps:

- Updating the Document Version table at the top of this page;
- Updating the relevant provision in this Plan;
- Replacing the updated version of the Plan eg. shared drives, Intranet;
- Printing a hard copy of the updated Plan for the office;
- Communicating the changes to all staff; and
- Archiving the old version of Plan.

References and related documents

Document Title
Risk Management Framework
Security Policy and Procedures Manual

Section 1 Introduction

Femili PNG assists survivors of family and sexual violence in Papua New Guinea. These services rely on infrastructure, including physical assets such as buildings for offices or safe houses, and non-physical assets such as data collected from clients and relationships within the community. Staff on the ground in PNG use these assets to facilitate services for clients.

All of these elements can be affected by disruption. Disruptions can be local, regional, or global, particularly as operations span two countries. Looking forward, Femili PNG prepares for disruptions in order to provide continuity and assurance to clients who require help.

The ability of any organisation to withstand disruption, and to function as close to capacity as possible, during times of crisis depends on the quality of preparation, planning for recovery, and the execution of these plans. In this way, 'organisational resilience' not only affects Femili PNG and staff, but critically, the survivors who Femili PNG support. It is at the time of heightened need in the community that organisations like Femili PNG are likely to have its capacity limited.

This Plan follows a PRR Framework: Prevention, Preparedness, Response and Recovery.

- Prevention - Risk Management planning
 - Incorporates the Prevention element that identifies and manages the likelihood and/or effects of risk associated with an incident.
- Preparedness - Business Impact Analysis
 - Incorporates the Preparedness element that identifies and prioritises the key activities of a business that may be adversely affected by any disruptions.
- Response – Incident Response planning
 - Incorporates the Response element and outlines immediate actions taken to respond to an incident in terms of containment, control and minimising impacts.
- Recovery - Recovery planning
 - Incorporates the Recovery element that outlines actions taken to recover from an incident in order to minimise disruption and recovery times.

1.1 Objectives

The purpose of developing this Business Continuity Plan is to ensure the continuation of business during and following any critical incident that results in disruption to normal operational capability.

The Objectives of this Plan are to:

- Understand the risks most likely to affect Femili PNG and continued operations
- Define and prioritise Femili PNG's critical business functions
- Detail the immediate response to a critical incidents
- Plan to continue and recover operations, including strategies and actions to be taken
- Review and update this Plan on a regular basis.

This Plan is devised in relation to identified disruptions that are likely to affect Femili PNG operations. However, it is noted that, during a crisis, specific operational planning will also be

undertaken. For example – for the COVID-19 pandemic, senior management planned according to alert levels as a dedicated response to the particular situation.

1.2 Glossary

Business Continuity Planning	A process that helps develop a plan document to manage the risks to a business, ensuring that it can operate to the extent required in the event of a crisis/disaster.
Business Continuity Plan	A document containing all of the information required to ensure that the business is able to resume critical business activities should a crisis/disaster occur.
Business Impact Analysis	The process of gathering information to determine basic recovery requirements for your key business activities in the event of a crisis/disaster.
Continuity	Refers to Femili PNG’s ability to maintain essential operations, during and after the disruption. The basic element of continuity is to keep the essential functions of Femili PNG running and minimising the time spent recovering afterwards.
Disruption	Refers to a disaster, emergency, or crisis that has the potential to interrupt Femili PNG’s operation. This could be global or regional (such as influenza or earthquake) or could be as localised as a political protest escalating to violence. Disruption can affect only one component of the organisation’s infrastructure or could affect every facet of it.
Key business activities	Those activities essential to deliver outputs and achievement of business objectives.
Recovery Time Objective (RTO)	The time from which a crisis/disaster is declared to the time that the critical business functions must be fully operational in order to avoid serious loss.
Resources	The means that support delivery of an identifiable output and/or result. Resources may be money, physical assets, or most importantly, people.
Risk Management	The process of defining and analysing risks, and then deciding on the appropriate course of action in order to minimise these risks, whilst still achieving business goals.

Section 2 Risk Management Planning

Femili PNG has a robust risk management planning process in place, and identifies, rates and mitigates all enterprise risks in Femili PNG's Risk Management Framework. Board and senior management review the Risk Management Framework every year

Femili PNG's existing risk management planning process are not replicated here. However, the following risks have been identified as potentially affecting Femili PNG's business continuity:

- natural disaster
- pandemic
- political instability
- civil unrest
- cyberattack.

The five main risks outlined above also pose the most credible threat to Femili PNG's operations as these disruptions have already affected past operations. While the risks associated with these disruptions cannot be eliminated, mitigations can be put in place and planning activated.

For details on how these risks have been identified, rated and mitigated, refer to Femili PNG's Risk Management Framework.

Section 3 Business Impact Analysis

As part of the Business Continuity Plan, Femili PNG has undertaken a Business Impact Analysis to assess the identified risks in Section 2 and their impacts in relation to critical business activities to determine basic recovery requirements.

The following are defined as key business activities that Femili PNG will attempt to continue in the event of a disruption:

- Case management services
- Emergency accommodation for clients
- Essential governance, security and logistical support
- Communications.

Overriding these key business activities is the need to ensure staff and client safety. The safety of staff will be prioritised over maintaining primary business function.

Below is the impact analysis of each of the identified possible disruptions to FPNG's work.

3.1 Natural disaster

Impact analysis - *High probability, high severity.*

PNG is particularly susceptible to natural disaster, alone accounting for 25% of all of the natural disasters in the Pacific between 1950 and 2008.¹ According to the UN Development Program, PNG experiences 2-3 large disasters each year, as well as additional, localised disasters which can be devastating to the communities affected. PNG is particularly prone to earthquakes, volcanic eruptions, tsunamis, cyclones, river flooding, coastal erosion, and landslides, all of which pose issues for Papua New Guineans directly or indirectly affected.

¹ https://www.pg.undp.org/content/papua_new_guinea/en/home/operations/projects/crisis_prevention_and_recovery/disaster-risk-management.html

The national government has recently scaled-up its disaster risk management effort, however the institutional capacity to respond to risks is still developing.² This is due to a combination of factors, including:

- the scale and frequency of disasters in the region
- a decentralised population over a large and geographically diverse area
- high poverty rates in the population and restricted government internal revenue with a reliance on external funding, and
- the need for long-term risk mitigation plans, rather than an emphasis on crisis response.

For Femili PNG, the short-term risks are similar to that of any organisation of a similar size, directly or indirectly affected by the disaster itself or disruption to supplies and communication. In the medium- to long-term, Femili PNG would be uniquely affected by a potential increase in client needs while restoring operations and services to their prior capacity if damaged. Funding through aid may also be affected by a natural disaster which demands resources to address.

Staff

Staffing may be immediately impacted by a natural disaster for the purpose of safety, care for family members, or property damage. Travel to and from Femili PNG's offices may be affected, limiting the capacity for services. Long-term property damage, injury, or affected family may mean that staff are unable to work at full capacity or at all. This may limit the capacity of Femili PNG overall, particularly if multiple staff are affected.

Case management services / Emergency accommodation for clients

The case management centres (CMCs) and safe house may be directly affected by damage. Damage to the CMCs may mean that services are halted or reduced, especially if buildings are considered unsafe. Capacity of safe houses may be reduced due to damage, safety requirements, and staffing. Demand for shelter may increase with referrals limited to high risk cases.

Essential governance, security and logistical support

Governance, security and logistical support is likely to be interrupted in a natural disaster. Due to infrastructure damage, staff may not be able to use phones or computers or access files. The CMC and safe house security systems may go down, placing staff and clients at risk. Lack of security may mean that resources and supplies are in higher demand than usual. Supplies may be interrupted.

Communication

Communication chains are likely to be interrupted in a natural disaster. Particularly, damage to telecommunications can prevent contact to other PNG- and Canberra-based staff.

Femili PNG's client survey system for data collection is designed for offline use, stored locally and uploading information at a later time. This process is unlikely to be strongly affected unless devices are damaged.

3.2 Pandemic

Impact analysis - *Medium probability, high severity.*

Pandemics are infrequent but can be devastating. Notably, the recent COVID-19 (coronavirus) pandemic in 2020 was a demonstration of the rapidness of the spread of a virus in an

² <https://www.gfdr.org/sites/gfdr/files/region/PG.pdf>

increasingly interconnected world. Pandemics by necessity will also disproportionately affect nations with a lack of healthcare infrastructure, such as PNG.

In the event of a global or regional pandemic, these events can affect Femili PNG's operations in two distinct ways. The first is the health impacts of disease, and the requirement of Femili PNG to implement safety measures for clients and staff, such as social distancing and limiting the capacity of safe houses. The second is the broad public policy issues which affect the context in which Femili PNG operates. This may include the effects of enforced restrictions of movement on the ability to repatriate clients, the increase in FSV that may occur, funding restrictions, or unrest that may occur if there are resource shortages.

Though they are regular occurrences, pandemics are considered 'medium-probability' for the purposes of planning due to the length of time in between occurrences. Though organisations of Femili PNG's size can make reasonable plans for response, much of the coordination will necessarily be done reactively to public policy changes and requirements.

For additional information about specific policies implemented during a pandemic, refer to the COVID-19 Alert Level Plan, produced in response to ongoing policy and safety requirements.

Staff

Staffing will be immediately impacted by a pandemic for the purpose of safety, requiring non-essential staff travel to be cancelled. Staff travel must include public transport. Depending on the scope of direct impact of the pandemic in PNG, staff safety may need to be prioritised, particularly those who may be more susceptible to illness.

Case management services / Emergency accommodation for clients

Depending on the nature of the pandemic, it is likely that CMC and safe accommodation would be severely affected. Client intake would necessarily be reduced, both for staff/client safety and organisational capacity with reduced staffing. Isolation and distancing requirements will need to be enforced as per requirements. Capacity of safe houses will be restricted and referrals limited to high risk cases.

Essential governance, security and logistical support

It is likely that certain governance, security and logistics functions would be affected by pandemic. Depending on the availability of internet connections, the governance may be least affected due to continued communication and access to Dropbox files. Security and logistics will be most affected. Security personnel may need to monitor staff/clients for symptoms and enforce distancing and/or other measures. Lack of security may mean that resources and supplies are in higher demand than usual. Supplies may be interrupted.

Communication

Communication chains are unlikely to be interrupted in a pandemic.

3.3 Political instability

Impact analysis - Low probability, medium severity

Political stability refers to the capacity for longevity and sustainability of institutions of governance. More broad than political violence and distinctly from civil unrest, political instability includes consideration of accountability, government effectiveness, regulatory quality, rule of law, corruption, as well as political violence.³

Political instability resulting in severe disruption to Femili PNG's operation specifically is relatively unlikely. Recently the 2011-12 constitutional crisis challenged provisions of the legal

³ World Bank via <https://www.encyclopedia.com/social-sciences/applied-and-social-sciences-magazines/political-instability-indices>

system on partisan lines, though no violence resulted. The 1997 Sandline Affair and Bougainville independence movement have seen sustained tensions and violence, though this has largely been concentrated on Bougainville Island.

Political stability/instability is the practical context in which Femili PNG operates, which as an organisation that necessarily works with government and its institutions such as the police, the legal system, or regulation. It also refers to the political landscape of PNG where it may affect operations or provide uncertainty as to the reliability of the institutions that Femili PNG utilises in the future.

For policies relating specifically to terrorism, consult the Security Manual.

Staff

It is likely that with governance instability broadly, staff capacity would not be acutely affected beyond the organisation's need to plan around uncertainty. However staffing could be impacted by a severe instance of political instability, where necessary government services fail, including healthcare, public transport, and policing/security.

Case management services / Emergency accommodation for clients

As with staff, it is unlikely that CMCs or the safe house would be directly affected by long-term issues of governance. Acute or severe instances of instability may directly affect the CMC or safe houses where Femili PNG interacts with government services, such as policing and the legal system.

Essential governance, security and logistical support

Resources are most likely to be affected, directly or indirectly by long-term political instability. Directly, this may be in the form of reduced funding availability, or a need for additional spending on security and other services. Indirectly, instability can broadly affect business supply chains and the availability of resources that Femili PNG requires to function. Security may also be a major concern, especially if political instability has a knock-on effect resulting in civil unrest, rioting, or increased criminal activity.

Communication

Communication are unlikely to be affected unless there is an acute instability that threatens to prevent existing digital/electronic communication infrastructure from functioning.

3.4 Civil unrest

Impact analysis - *Medium probability, high severity*

Distinct from political instability, civil unrest can include violence or threat of violence for a variety of reasons, including resource scarcity due to one of the above disruptions. Though civil unrest is often political, it is not necessarily so. The threat of violence as a unique issue should be distinguished and addressed separately to, for example, long-term issues of governance and its effects on operations.

Two primary issues should be in consideration when planning for continuity of operations around potential civil unrest: the responding to the threat of violence in a riot and government response to the violence.

Recent examples include the declaration of a state of emergency, suspension of provincial government, and law enforcement by PNG military in response to 2018 riots in the Southern Highlands.⁴ The riots were in response to an election dispute and resulted in a warehouse of food supplies being taken and burning of property, including a plane and buildings in Mendi. After the 2018 Southern Highlands riots, a state of emergency was declared by government for nine months in response.

For policies relating specifically to terrorism, consult the Security Manual.

Staff

Staff are more likely to be directly impacted by civil unrest than ongoing structural issues of political instability, noting particularly that even localised unrest has the capacity to disrupt individual staff members or operations heavily. Personal impact by violence or threat of violence has the capacity to severely disrupt staff capacity and threaten safety. Staff may have difficulty attending work due to restrictions of movement.

Case management services / Emergency accommodation for clients

As with staff, case management services and safe houses may be directly affected both to operations and demand for services. Freedom of movement may be impeded, resulting in survivors being unable to access services.

Essential governance, security and logistical support

Resources are most likely to be affected, directly or indirectly, by long-term unrest. Directly, this may be in the form of reduced fund availability or a need for additional spending on security. Indirectly, civil unrest can broadly affect business supply chains and subsequently the availability of resources that Femili PNG requires to function. Security will also be affected by civil unrest, placing staff/clients at greater risk.

Communication

Communication chains may be affected depending on the effect of the disruption on staff. If staff are not directly affected, communication capacity is unlikely to be reduced unless there is an event that threatens to prevent existing digital/electronic communication infrastructure from functioning.

3.5 Cyberattack

Impact analysis - *Medium probability, high severity.*

A cyberattack is an assault launched by cybercriminals using one or more computers against a single or multiple computers or networks. A cyberattack can maliciously disable computers, steal data, or use a breached computer as a launch point for other attacks. Since COVID-19,

⁴ <https://www.abc.net.au/news/2018-06-16/papua-new-guinea-declares-state-of-emergency-over-riots/9877830>

there has been a marked increase on the numbers of NGOs that have been subject to cyberattacks and phishing attempts.⁵ This increase has been as a result of more remote working, and increased vulnerabilities that cyber criminals have sought to exploit.

Common types of cyberattacks include (but not limited to):⁶

- **Malware:** malicious software, including spyware, ransomware, viruses, and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software.
- **Phishing:** the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine. Phishing is an increasingly common cyberthreat.
- **Denial-of-service:** A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests.

For Femili PNG, the short-term risks are similar to that of any organisation of a similar size, with immediate disruption to essential governance, logistics and communication. In the medium- to long-term, Femili PNG may be affected financially or reputationally, if information is stolen and released, ransomware installed, or bank or other financial information is harvested and used to break into bank accounts.

Staff

Staffing may be immediately impacted due to their inability to access IT to continue working. Staff personal information may also be unlawfully accessed as a result of a hack. However, a cyberattack is unlikely to threaten staff physical health and safety.

Case management services / Emergency accommodation for clients

The CMCs and safe house may be affected in that their internet, email and IT access will be curtailed for a period of time in the event of a cyberattack. However, case management functions can be conducted offline, so effects could be limited. The loss of court documents or client statements may be a possibility and may create delays.

Essential governance, security and logistical support

Governance, security and logistical support is likely to be substantially interrupted in a cyberattack. Depending on the type of attack, staff may not be able to use phones or computers or access files or email. Payment and filing systems may be compromised, leading to money and information being stolen and staff locked out of files.

Communication

Communication chains will be substantially interrupted in a cyberattack. All email and internet-based communications will be affected, as well as phones, in some instances.

Femili PNG's client survey system for data collection is designed for offline use, stored locally and uploading information at a later time. All client data is password-protected and stored securely. This process is unlikely to be strongly affected unless keystroke recognition malware is launched on a computer from which this information is accessed.

⁵ www.devex.com/news/covid-19-brings-wave-of-cyberattacks-against-ngos-96934

⁶ www.cisco.com/c/en_au/products/security/common-cyberattacks.html#~types-of-cyber-attacks

3.5 Business Impact Analysis

Critical Business Activity	Description	Priority	Impact of loss <i>(describe losses in terms of financial, staffing, loss of reputation etc)</i>	RTO <i>(critical period before business losses occur)</i>
Case management services	Provision of case management services to survivors of FSV.	High	<ul style="list-style-type: none"> • survivors cannot readily access services • law and justice interventions are delayed or unavailable • access to medical services and safe accommodation impeded • funding affected as not meeting deliverables or providing promised services. 	2 weeks
Emergency accommodation	Provision of emergency accommodation for high-risk survivors of FSV.	High	Survivors and their dependents at high risk of serious injury, death or homelessness.	1 day
Essential governance, security and logistics	The governance, security and logistics functions which are necessary to support the delivery of case management and safe accommodation services.	High	<ul style="list-style-type: none"> • unable to carry out governance support function • security issues putting staff and clients at risk • unable to obtain resources such as basic necessities for clients. 	2 weeks
Communication	The ability of FPNG stakeholders to communicate with each other – staff, clients, service providers, funders, etc – through phone or email.		<ul style="list-style-type: none"> • Unable to provide updates • Unable to monitor staff and clients • Unable to communicate problems • Unable to seek help or emergency assistance. 	1 day

Section 4 Incident Response Plan

This section sets out the immediate response required to the possible identified disruptions. Further details on immediate response are in the Security Manual.

4.1 Natural disasters

Earthquake

If you are indoors during an earthquake:

- Drop to the ground.
- Take cover by getting under a sturdy table or other piece of furniture and hold on until the shaking stops. If there isn't a table or desk near you, cover your face and head with your arms and crouch in an inside corner of the building.
- Stay away from glass, windows, outside doors and walls, and anything that could fall, such as lighting fixtures or furniture.
- Do not use a doorway except if you know it is a strongly supported, load-bearing doorway and it is close to you.
- Stay inside until the shaking stops and it is safe to go outside. Do not exit a building during the shaking.

If you are outdoors during an earthquake:

- Stay there.
- Move away from buildings, streetlights, and utility wires.
- Once in the open, stay there until the shaking stops.

Floods, damaging winds and rain

If you are in the office, and there is a risk of flooding and damaging rains:

- Stay updated about the weather through news services and radio.
- Move any items or furniture up high to avoid flooding and away from any leaks. Putdown containers to catch any leaks. Ensure all windows are closed.
- Consider the need to send staff home if it is safe to do so, and if they are in danger of being cut off from their homes.

If staff are at home and there is the danger of flooding and damaging rains:

- Stay updated about the weather through news services and radio.
- If you are concerned about leaving home to come to work, contact the Logistics and Security Officer and Operations Director for advice.

4.2 Pandemic

Responding to a pandemic is necessarily reactive to extrinsic events rather than as a result of comprehensive planning. As a result, responses are coordinated around the judgement and capacity of staff and leaders, planning communication chains, and health/hygiene procedures. Advice from the World Health Organization and the Governments of PNG and Australia will be followed.

Pandemics by nature may not require an immediate response in the same way as a natural disaster or violence, but rather ongoing monitoring of risks and decision making appropriate. As an example, see the Alert Level planning conducted for COVID-19.

4.3 Political instability

Past political instability in PNG has led to rioting and acts of violence. Responding to potential political instability is necessarily reactive to extrinsic events rather than a result of comprehensive planning. As a result, responses are coordinated around the judgement and capacity of staff and leaders, planning crisis communication chains, and security procedures. The Security Manual should be consulted for in-depth responses to specific scenarios related to targeted violence.

If a significant political event occurs, such as a change of leadership or act of violence against a political leader:

- Monitor reports of rioting and violence in your area.
- If there is rioting in your area and you are in a safe place, do not leave, stay in place.
- Contact the Logistics and Security Officer to let them know of your location.
- If there is rioting in your area and you are not in a safe place, seek shelter where you will be safest, for example a police station or building with security guards.
- Where the rioting or violence occurs near the Femili PNG CMC or Safe House, lockdown procedures will be observed and staff will not leave until it has been deemed safe by the Logistics & Security Officer, Operations Directors and CEO.
- Where staff are at direct risk or injured from rioting caused by political instability, the event shall be managed according to critical incident management protocols.

4.4 Civil unrest

As with political instability, responding to civil unrest is necessarily reactive to extrinsic events rather than as a result of comprehensive planning. As a result, responses are coordinated around the judgement and capacity of staff and leaders, planning crisis communication chains, and security procedures. A key difference between response to civil unrest and political instability is the prolonged nature and uncertainty that comes with political instability. The Security Manual should be consulted for in-depth responses to specific scenarios related to targeted violence.

There are two issues that should be addressed when determining Femili PNG's response to civil unrest: the immediate threat of violence from a riot, and planning around the state response to the threat of violence.

If a significant event of civil unrest occurs, such as riots, violence, or looting in an area in proximity to a Femili PNG office:

- Monitor reports of rioting and violence in your area.
- If there is rioting in your area and you are in a safe place, do not leave and stay in place.
- Contact the Logistics and Security Officer to let them know of your location.
- If there is rioting in your area and you are not in a safe place, seek shelter where you will be safest, for example a police station or building with security guards.
- Where the rioting or violence occurs near the Femili PNG CMCs or Safe House, lockdown procedures will be observed and staff will not leave until it has been deemed safe by the Logistics and Security Officer, Operations Directors and CEO.
- Where staff are at direct risk or injured from rioting caused by political instability, the event shall be managed according to critical incident management protocols.

4.5 Cyberattack

The response to a cyberattack will be dependent on the type of attack, its source, and how the attack occurred. It may not be possible to tailor a response until this is known. However, immediate steps in the event of a cyberattack include:

- Inform EMC and the IT Manager by WhatsApp of the attack, and all managers to inform their staff to immediately log off their email / internet and disconnect their computers.
- All passwords are changed, including staff email and dropbox.
- Anti-virus scans are run on all dropbox files.
- If a phishing attack, relevant spam and global filters applied. Server host contacted to locate source of the attack.
- Immediately inform all affected stakeholders, warning them to beware communications from Femili PNG.
- Obtain professional IT support on the ground in PNG or Australia, depending on where the attack's first entry point was.

Depending on the severity of the cyberattack, ongoing monitoring for a period of time after the immediate attack may be necessary.

4.6 Immediate Response Checklist

The below immediate Response Checklist may be used in the event of an emergency or disruption:

INCIDENT RESPONSE	ACTIONS TAKEN
Have you:	
• assessed the severity of the incident?	
• evacuated the site if necessary?	
• accounted for everyone?	
• identified any injuries to persons?	
• contacted Emergency Services?	
• implemented your Incident Response Plan?	
• started an Event Log / documented in Incident Register?	
• activated staff members and resources?	
• gained more information as a priority?	
• briefed team members on incident?	
• allocated specific roles and responsibilities?	
• identified any damage?	
• identified critical activities that have been disrupted?	
• kept staff informed?	
• contacted key stakeholders?	
• understood and complied with any regulatory/compliance requirements?	

4.7 Evacuation procedures & Emergency kits

Evacuation Plans are on display and accessible to all staff in Lae, Port Moresby and Canberra. Emergency kits are maintained and include:

Documents:

- Business Continuity Plan – your plan to recover your business or organisation in the event of a critical incident.
- List of employees with contact details.
- Contact details for emergency services.
- Latest asset register.
- Insurance details.
- Financial and banking information.

Equipment:

- Computer back-up tapes/disks/USB memory sticks or flash drives.
- Spare keys/security codes.
- Torch and spare batteries.
- General stationery (pens, paper, etc).
- Mobile telephone with credit available, plus charger.
- Dust and toxic fume masks.

4.8 Roles and Responsibilities

In the event of an emergency or disruption, the communication and notification procedures in these sections will be followed. The EMC, CEO, Development Manager, or Operations Directors can activate the Business Continuity Plan.

Key Contact Sheet

Contact List – Internal

Lae Office

Femili PNG Case Management Centre, C/-Lutheran Social Concern Building, Section: 6, Lot: 28, Top Town, Lae, Morobe.

- CEO: +675 7274 6258.
- CEO's home address: Unit 9, Allotment: 30, Section: 32, Lot Oleander Avenue, Eriku Lae, Morobe.
- Operations Director: +675 7091 4031
- Security/Admin and Logistics Support Officer: +67570804628
- Administrator: +675 70914028

Port Moresby Office

Femili PNG Case Management Centre, Unit 1B, Datec Office Complex Section: 57, Allotment 4-10 Hohola Port Moresby, National Capital District.

- CEO: +675 7274 6258
- Operations Director: +675 72145728/75242478
- Security/Admin and Logistics Support Officer: +675 7216 7383
- Administrator: +675 70307979/ 75630117

Goroka Office

- CEO: +675 72746258
- Operations Manager: +675 74967280
- Security and Logistics Officer: +675 72068720
- Admin/ Information Officer: +675 70876296

National Office

Femili PNG National Office, First Floor SVS Compound, Mangola Street near/opp Brian Bell Plaza, Lae, Morobe

- HR Manager: +675 7022 6482
- Finance/Admin Coordinator: +675 7091 4028
- IT Manager: +675 72991444

Contact List – External

Guard Dog Security Services

- POM Guard Dog Security Services: +675 7202 9653.
- Lae Guard Dog Security Services: +675 7372 709 or +675 7373 2490.

Ambulance services:

- Lae Wellness Clinic 24/7 contact number: +675 472 777 or Dr Solano: +675 7122 5450
- Lae International Ambulance Service: +675 7190 2700.
- POM Pacific International Hospital, 24/7 contact number: +675 7998 8000 / 7111 4000.
- POM St. Johns Ambulance Service: +675 7111 1234.

Communication and notification

In the event of a major disruption, the communication response is the same as a security incident. The immediate communication reporting chain is as follows:

1. **Report incident to the CEO, Daisy Plana (+675 7274 6258).**
If the CEO is unavailable or the CEO is involved in the incident, report to the relevant Operations Director/Manager and other EMC staff:
2. CEO (or Operations Director or Security/Admin and Logistics Support Officer or another staff member if Operations Director and Security/Admin and Logistics Support Officer are unavailable) to contact:
 - **Femili PNG Chair Stephen Howes (+61 400 167 936).**
3. The CEO (or the alternate) will then:
 - Initiate immediate essential response to prevent further harm to victims. This may include medical response or extraction by Police or Guard Dog Security Services.
 - Write incident report, after the immediate essential response has occurred.

- Start logbook.
- Where appropriate, inform trusted authorities who are considered willing to assist.

Further detail about security incidents should consult the Security Policy and Procedures Manual.

Section 5 Recovery

This section outlines Femili PNG's recovery, or long-term response, to disruptions.

5.1 Natural disasters

To facilitate recovery from a natural disaster:

- **Staff:** Ultimately, staff and client safety is the primary concern of Femili PNG. Staff personally affected are given as much time as reasonably possible to recover. For staff unaffected directly, flexibility may be required to ensure client assistance and safety by covering shifts. Where travel to and from Femili PNG's office is restricted, management should coordinate directly with staff about an appropriate response, which may include arranging transportation for staff to/from the office.
- **Case management services / Emergency accommodation for clients:** Where the CMC or safe house is damaged, the extent of the damage should be assessed in order to prevent harm to staff and clients. Should a CMC/safe house have to shut due to damage, the relevant manager should first seek to coordinate with other local safe houses in order to secure accommodation for high-risk clients. For damage to the CMC, alternate working arrangements (ie, staff working from home or another location) should be made. Staff should only enter the CMC/safe house once it has been declared structurally sound and it is safe to do so.
- **Essential governance, security and logistical support:** After a natural disaster, essential resources may be in higher demand and lower supply than usual. Supply chains may also be disrupted, restricting access to essential supplies. Management should continue to monitor access to supplies and attempt to purchase supplies and emergency supplies in advance.
- **Communication:** Affected telecommunications infrastructure means that information/communication chains would probably be immediately interrupted. Staff to continue to try to make contact however possible without putting themselves at risk/danger.

5.2 Pandemic

To facilitate recovery from a pandemic:

- **Staff:** Staff that are not required to work in-person should not be required to come into the office. If appropriate, shifts to work around public transport to avoid staff travel on crowded buses or alternate transportation arranged for staff. Regular screening of staff and clients, enhanced hygiene procedures, social distancing and regular updates on procedures will be observed.
- **Case management services / Emergency accommodation for clients:** All clients to be screened prior to admission and potentially infected clients to be isolated to control infection possibility. Constant/regular disinfecting of common areas (as relevant).
- **Essential governance, security and logistical support:** Relevant resources to be stocked where the potential for a pandemic arises, including all purchases, supply and emergency items.

- **Communication:** Development of a formal response plan for staff and external stakeholders. Coordination of communication chains for relevant virus updates or public policy developments.

5.3 Political instability

To facilitate recovery from political instability:

- **Staff:** Staffing of office and safe houses may not be directly affected by minor issues of governance instability. For severe issues, staffing may be reduced, increased security may be provided, and transport to/from work may be provided for safety.
- **Case management services / Emergency accommodation for clients:** CMCs and safe houses will largely retain their operation as normal. Increased security may be provided as relevant. Change in operations will be done with respect to staff and client safety where government services fail to provide services required at the direction of the EMC and centre management.
- **Essential governance, security and logistical support:** Relevant resources to be stocked where the potential for a severe instance of instability arises, including all purchases, supply and emergency items, at the direction of the EMC. Additional security and logistical support may be required in the short term.
- **Communication:** Coordination of communication chains for relevant developments. Development of a formal response plan for staff and external stakeholders.

5.4 Civil Unrest

To facilitate recovery from civil unrest:

- **Staff:** Staffing of CMC and safe house may not be impacted long-term by localised instances of civil unrest. However response to instances of civil unrest where operations and staff have the potential to be directly affected may necessarily involve reduced staffing, increased security, and/or providing transport for staff working for safety. Alternate working conditions, such as working from home, may be considered in the short-term.
- **Case management services / Emergency accommodation for clients:** Safe houses may be directly affected by instances of civil unrest, both to operations and demand for services. Increased security should be provided as relevant. Change in operation will be done with respect to staff and client safety where government services fail to provide services required as per the direction of the EMC and local safe house management.
- **Essential governance, security and logistical support:** Relevant resources to be stocked where the potential for a severe instance of instability arises, including all purchases, supply and emergency items, at the direction of the EMC. Additional security and logistical support may be required in the short term.
- **Communication:** Coordination of communication chains for key, up-to-date changes. Development of a formal response plan for staff and external stakeholders.

5.5 Cyberattack

To facilitate recovery from a cyberattack:

- **Staff:** When the attack is over and their computers have been checked, staff can be slowly given IT access and brought back online when it is safe to do so. A risk approach can be taken to this, ie – the least affected can be brought online first; the most affected last. A report on the attack, and any recommendations, should

be shared with staff to increase understanding of online safety and how attacks can be prevented in the future.

- **Case management services / Emergency accommodation for clients:** During recovery, consideration is given to how the cyberattack has affected case management services / emergency accommodation (if any). Clients with pending cases to be followed-up in the event that their documents have not been received. Any clients whose data may have been compromised are contacted.
- **Essential governance, security and logistical support:** Suppliers and contacts are informed of the attack and are advised to re-send any invoices/other important documentation, so that supply is not interrupted. Ongoing monitoring of files, with regular anti-virus scans, to ensure no malware has been deployed in the essential files of the organisation. Manual back-ups of files are conducted.
- **Communication:** Report on attack is shared with all staff, as awareness-raising activity. Funders and stakeholders are advised on the attack, and any other relevant information. In some circumstances, public communication via website and social media will be appropriate.

5.6 Recovery Plan

Key Business Activities	Preventative/Recovery Actions	Resource Requirements/ Outcomes	Recovery Time Objective	Responsibility
Case management services	<ul style="list-style-type: none"> • triage new clients into high and low risk, and those needing immediate interventions • Source alternative working arrangements where necessary, ie – caseworkers working from home or other location • Determine capacity of service providers and plan accordingly 	<ul style="list-style-type: none"> • Emergency funding to cover costs of disruption • Reliable and secure IT and telecommunications technologies • Emergency supply of basic necessities and non-perishable food. • Important files and documents stored on Dropbox 	2 weeks	EMC, Casework team
Emergency accommodation	<ul style="list-style-type: none"> • triage clients that are high risk and needing immediate safety and security • Determine capacity of safe house service providers and plan accordingly • Use back-up option of paid accommodation for short-term intervention 	<ul style="list-style-type: none"> • Emergency funding to cover costs of paid accommodation • Good relationships with safe houses • Back-up paid accommodation 	1 day	EMC, Casework team
Essential governance, security and logistics	<ul style="list-style-type: none"> • Determine recovery security and logistical needs and plan accordingly • Ensure security systems are operational at CMC/safe house • Ensure supplies of basic necessities for clients • Check damage to assets including vehicles and file appropriate insurance claims • Determine access to important governance functions such as MYOB, payroll, files and documents. 	<ul style="list-style-type: none"> • Emergency funding for security and necessities • Back-up security systems • Reliable and secure IT and telecommunications technologies • Important files and documents stored on Dropbox 	2 weeks	EMC, Security & Logistics Officers
Communication	<ul style="list-style-type: none"> • Where possible, telecommunications are re-established as a priority • Communications established with service providers, funders and between Lae, POM and Canberra offices • Services able to be offered by FPNG are communicated through website, social media/other means. 	<ul style="list-style-type: none"> • Reliable and secure IT and telecommunications technologies • Important files and documents stored on Dropbox 	1 day	EMC, Communications Officer, Security & Logistics Officer

5.7 Incident Recovery Checklist

Below is an Incident Recovery Checklist for use when entering the Recovery phase.

INCIDENT RESPONSE	ACTIONS
Now that the crisis is over have you: <ul style="list-style-type: none"> • refocused efforts towards recovery? 	
<ul style="list-style-type: none"> • redeployed staff members and resources as necessary? 	
<ul style="list-style-type: none"> • continued to gather information about the situation as if effects you? 	
<ul style="list-style-type: none"> • assessed your current financial position? 	
<ul style="list-style-type: none"> • reviewed cash requirements to restore operations? 	
<ul style="list-style-type: none"> • contacted your insurance broker/company? 	
<ul style="list-style-type: none"> • kept staff informed? 	
<ul style="list-style-type: none"> • kept key stakeholders informed? 	
<ul style="list-style-type: none"> • set priorities and recovery options? 	
<ul style="list-style-type: none"> • updated the Recovery Plan? 	
<ul style="list-style-type: none"> • captured lessons learnt from your individual, team and business recovery? 	

5.8 Recovery contacts

In the event of a disruption, the following contacts list will be created and updated as recovery contracts are made and recovery actions occur. The categories below are a guide, new contacts and categories can be added according to the specific recovery actions undertaken.

Contact Type	Organisation Name	Contact	Phone / Mobile / Email	Notes
Insurance				
Telephone/ISP				
Bank				
Suppliers				
Suppliers				
Accountant				
Funders				
Landlord				

5.9 Insurance claims

In the event of a disruption, the following insurance claims list will be created and updated as insurance is claimed in respect of recovery actions. New insurance claims can be added according to the specific recovery actions undertaken.

Insurance company	Date	Details of claim	Follow-up actions
ABC Insurance	00/00/00	Enter details of claim and contact person.	Actions required by the insurer to process claim, eg photos, damage estimates

Section 6 Preparation & Prevention

While it is impossible to prevent the disruptions that pose a threat to Femili PNG's operations, it is possible to prepare for them. Below are some of the proposed preparation strategies.

6.1 Natural disasters

- **Staff:** Staff are trained on immediate emergency procedures, including familiarity with exits, procedures, and any risks.
- **Case management services / Emergency accommodation for clients:** CMCs/safe houses are equipped with all reasonable emergency supplies. Where notified of a risk, management to direct precautionary measures, such as reinforcing windows, moving furniture and moving clients to safe locations.
- **Essential governance, security and logistical support:** Where there is a heightened threat of a natural disaster, resources should be purchased in preparation. As directed by management in response to news updates, safe houses and CMCs may be directed to complete stock in advance for all emergency, purchase, and supply resources.
- **Communication:** Relevant risks to Femili PNG offices or safe houses should be communicated in advance where possible. When this option is unavailable, such as earthquakes, management should contact EMC, CEO and/or Security & Logistics Officer as soon as possible.

6.2 Pandemic

- **Staff:** The speed of response required to a pandemic relative to other risks means it is appropriate for the EMC to implement Alert Level planning in response to the particular conditions of the pandemic.
- **Case management services / Emergency accommodation for clients:** CMC/safe house preparation will be in response to public policy and staff safety requirements as designated by the EMC.
- **Essential governance, security and logistical support:** Resource preparation is the most critical element of response to a pandemic. As directed by the EMC in response to policy developments or news updates, safe houses and CMCs may be directed to complete stock in advance for all emergency, purchase, and supply resources.
- **Communication:** Communication chains for updates should be developed in response to an alert or a risk identified by the EMC.

6.3 Political Instability

- **Staff:** Staff safety is paramount, but the extrinsic nature of instability means that policies and procedures must be developed in response to specific events as they happen. The EMC and senior staff should be prepared and informed on potential governance issues which pose a threat to Femili PNG's operations. Information should be provided to front-line staff when onboarding. Any issues of safety and security will be communicated to staff.
- **Case management services / Emergency accommodation for clients:** CEO has discretion to make decisions rapidly for the safety of staff and clients. Planning should be made by the EMC in coordination with staff.

- **Essential governance, security and logistical support:** Relevant resources to be stocked where the potential for a severe instance of instability arises, including all purchases, supply and emergency items, at the direction of the EMC.
- **Communication:** Coordination of communication chains for relevant developments, particularly for on-ground staff to EMC for up-to-date information and local assessment of risks.

6.4 Civil Unrest

- **Staff:** Staff safety is paramount, but, as with political instability, the extrinsic nature of risk means that policies and procedures must be developed in response to specific events as they happen. The EMC and senior staff should be prepared and informed on potential issues of local unrest which pose a threat to Femili PNG's operations, as well as receive updates about key risks from staff. Any flagged workplace issues of safety and security will be communicated to staff.
- **Case management services / Emergency accommodation for clients:** CEO has discretion to make decisions rapidly for the safety of staff and clients. Planning should be made by the EMC in coordination with staff.
- **Essential governance, security and logistical support:** Relevant resources to be stocked where the potential for a severe instance of unrest arises, including all purchases, supply and emergency items, at the direction of the EMC and local management.
- **Communication:** Coordination of communication chains for relevant developments, particularly for on-ground staff to EMC for up-to-date information and local assessment of risks.

6.5 Cyberattack

- **Staff:** Staff are trained on IT security and how to identify scams. Staff personal information is stored securely.
- **Case management services / Emergency accommodation for clients:** Manual back-up of all client data and clients forms stored offline/ in hard copy.
- **Essential governance, security and logistical support:** Appropriate IT support and advice is sought and obtained. Server and email security is regularly upgraded. Software is kept up to date and patches applied. Passwords are changed regularly.
- **Communication:** As per essential governance, security and logistical support above. Senior management should also have access to multiple telecommunications – WhatsApp, mobile, landline, other email accounts – to communicate in the event of a cyberattack.

6.6 General preparations

General preparations to facilitate business continuity in the event of a disruption will include:

- Establishing and maintaining good relations with service providers
- Keeping staff contact lists updated
- Annual review of the Security Manual by senior management and the Board
- Regular review of the Business Continuity Plan (see 6.7)
- Keeping an appropriate level of operational reserves
- Ensure that the EMC, Security & Logistics Officers and IT Manager are familiar with the Business Continuity Plan and know how to activate it

- Staff refresher training on the Security Manual is provided annually for emergency and safety procedures
- Important files are stored on Dropbox with regular, manual and offline back-ups made.

6.7 Review schedule

Review date	Reason for review	Changes made
4.7.2020	<i>First review of draft Plan</i>	<i>Plan drafted</i>
1.5.2026	<i>Passage of time</i>	<i>Removal of Friends of Femili PNG (FPNGA); minor changes and updating</i>