CIM SECURITIES, LLC

BUSINESS CONTINUITY & DISASTER RECOVERY

P.O. Box 810, Willow, AK. 99688
Phone: 732-966-9244

BUSINESS CONTINUITY & DISASTER RECOVERY PLAN

1.01 INTRODUCTION

According to FINRA Rule 4370, CIM SECURITIES LLC ("CIM SECURITIES" or the "Company") must create and maintain a written business continuity plan, identifying procedures relating to an emergency or significant business disruption. Such systems must be reasonably designed to enable the Company to meet its existing customer obligations. The policies must address the Company's existing relationships with other broker-dealers and counterparties. The business continuity plan must be made available promptly upon request to FINRA staff.

The Company has created a business continuity and disaster recovery plan to protect the Company in the event of a catastrophe that would disrupt operations and cause a loss of vital information regarding our business and clients. These procedures will ensure the protection of the business records and our ability to recover and resume operations quickly.

CIM SECURITIES will maintain its plan by employing the following actions:

a. Periodically test the plan
b. Periodically review and revise the plan when necessary
c. Distribute the plan to key employees to maintain copies off-site.
d. Communicate the recovery plan to all employees.

CIM SECURITIES shall make a copy of all data vital to CIM SECURITIES operations weekly. The data to be copied includes the following:

a. CIM SECURITIES Accounting data
b. CIM SECURITIES Client Basic Information (see contact information in page footer)
c. CIM SECURITIES Corporate Documents

A copy of this data shall be kept outside of BD Main. All clients' trading information is kept online on a server with redundant backups.

All other financial information regarding bank accounts statements; a digital back-up also maintains client deposit history in Willow, AK.

Customer account documents will provide notice of a telephone number at which the customer could obtain information concerning their account in addition to the status of any trading activity in the event of a catastrophic event that requires implementation of the business continuity and disaster recovery plan.

The Compliance Offer has verified that the following clearing firms (N/A), liquidity providers, deposit banks, and other key counterparties for CIM SECURITIES have appropriate AML procedures.

CityWide Banks

1.02 MISSION STATEMENT & OBJECTIVE

In the event of a significant incident that affects or has the potential to affect the operations of the financial markets, CIM SECURITIES coordinates the business continuity planning efforts with the corresponding financial industry. These efforts are managed through the **Emergency Command Center** headed by the Chief Executive Officer of the Company, which identifies the status of industry participants, disseminates vital information and timely updates on the market's recovery, and facilitates actions to assist market participants in resuming their business. Coordination is arranged amongst our counterparties (liquidity providers and clearing firms), other financial firms (such as depository banks), relevant exchanges, industry utilities, regulators, and public sector emergency managers.

Our objective is to develop and test a well-structured and coherent plan that will enable the organization to recover quickly and effectively from an unforeseen disaster or emergency that interrupts normal business operations.

CIM SECURITIES' Board of Directors has approved the following:

- CIM SECURITIES should develop a comprehensive Business Continuity Plan.
- A formal risk assessment should be undertaken to determine the requirements for the Business Continuity Plan.
- The Business Continuity Plan should cover all essential and critical business activities.
- The Business Continuity Plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergencies and that the Management and staff understand how it is to be executed.
- All staff must be made aware of the Business Continuity Plan and their respective roles.
- The Business Continuity Plan is to be kept up to date to consider changing circumstances.

The following plan has been approved by the Board of Directors and is current as of October 7, 2025.

1.03 REQUIRED DOCUMENTS & INFORMATION

A Manager should prepare a list of all necessary documents and information for recovery in case of any disaster. The Company will store copies of these documents at an off-site location. Where this includes documents containing sensitive information, the Manager must take care to ensure that confidentiality is not compromised. Valid documents and data include the following:

- Organization chart showing names and positions
- Staff emergency contact information
- List of suppliers and contact numbers
- List of professional advisers and emergency contact information
- List of emergency services and contact numbers
- Premise address and map
- IT system specification
- Communication system specification
- Copies of maintenance agreements/service level agreements
- Existing evacuation procedures and fire regulations
- Health and Safety procedures
- Conduct of Business Procedures Manual

- Copies of floor plans
- Asset inventories
- Inventories of information assets
- IT inventories
- Relevant industry regulations and guidelines
- Insurance information
- Client Account Transaction History
- Client Account Activities

1.04 EMERGENCY INCIDENT ASSESSMENT

There are many potential disruptive events, and the impact and probability level must be assessed. It is, therefore, necessary to consider each potential disruptive threat. Potential Emergencies may be a result of one or more of the following disasters:

Probability Rating		**Impact Rating**	
Score	**Level**	**Score**	**Level**
1	Very High	1	Terminal
2	High	2	Devastating
3	Medium	3	Critical
4	Low	4	Controllable
5	Very Low	5	Irritating

Environmental Disasters

- **Flood** **Probability Rating: 5 Impact Rating: 5**

Floods result from thunderstorms, tropical storms, snow thaws, or heavy and prolonged rainfall causing rivers to overflow their banks and flood the surrounding areas. Floods can seriously affect buildings and equipment, causing power failures and loss of facilities and resulting in injury or death.

- **Snowstorm** **Probability Rating: 5 Impact Rating: 5**

Snowstorm conditions can include blizzards, strong winds, and freezing temperatures with significant amounts of snow. Snow and ice can impact power and communications, and employees may be unable to travel to work due to the impact on public transport or road conditions. Buildings can collapse under the weight of snow, and injuries or even death could occur through freezing temperatures and icy conditions.

- **Electrical storms** **Probability Rating: 4 Impact Rating: 4**

The impact of lightning strikes can be significant. It can disrupt power and can also cause fires. It may also damage electrical equipment, including computer systems. Structural damage is also possible through falling trees or other objects.

- **Fire** **Probability Rating: 4 Impact Rating: 4**

Fires are often devastating and can be started through a wide range of events which may be accidental or environmental. Deliberate fires caused by arson are dealt with in the topic (Organized and Deliberate Disruption). The impact on the business will vary depending on the severity of the fire and the speed at

which it can be brought under control. A fire can cause human injury or death, and damage can also be caused to records and equipment and the fabric or structure of premises.

- **Freezing Conditions** **Probability Rating: 5 Impact Rating: 5**

Freezing conditions can occur in winter periods, and the effects can be devastating. Where temperatures fall in excess of – 30 Centigrade, they can create conditions that significantly disrupt businesses and even cause death or injury. Businesses and homes can be seriously affected by burst pipes, inadequate heating facilities, and disruption to transport.

- **Epidemic** **Probability Rating: 5 Impact Rating: 5**

An epidemic can occur when a contagious illness affects many persons within a country or region. This can have a particularly devastating short-term impact on business through many persons being absent from work simultaneously. Certain illnesses can have a more prolonged-term effect on the business where long-term illness or death results. An example of this extreme situation is occurring in certain third-world countries where the Aids virus is considered to be of epidemic proportions.

Organized & Deliberate Disasters

- **Act of terrorism** **Probability Rating: 4 Impact Rating: 3**

Acts of terrorism include explosions, bomb threats, hostage-taking, sabotage, and organized violence. Whether this is perpetrated through a recognized terrorist organization or a violent protest group, the effect on individuals and business is the same. Such acts create uncertainty and fear and serve to destabilize the general environment.

- **Act of Sabotage** **Probability Rating: 4 Impact Rating: 3**

An act of sabotage is the severe, deliberate disruption of an organization's activities with an attempt to discredit or financially damage the organization. The business will often be immediately and seriously affected by successful sabotage. This can affect normal operations and also serve to destabilize the workforce. An internal attack on the IT systems through the use of malicious code can be considered to be an act of sabotage.

- **Act of war** **Probability Rating: 5 Impact Rating: 3**

An act of war is the commencement of hostilities between one country and another. This could take the form of air strikes, ground strikes, invasions, or blockades. Businesses could be immediately affected where they are either located near the outbreak of hostilities or dependent upon imports or exports for survival. Many businesses do not survive a prolonged outbreak of war.

- **Theft** **Probability Rating: 4 Impact Rating: 4**

This hazard could range from the theft of goods or equipment to the theft of money or other valuables. In addition to possibly financially damaging the organization, theft can cause suspicion and uncertainty in the workforce, where it may be believed that one or more of them could have been involved.

- **Arson** **Probability Rating: 5 Impact Rating: 3**

Arson is the deliberate setting of a fire to damage the organization's premises and contents. This can cause both loss of premises and goods and other assets, which can be highly disruptive to the organization.

- **Labor Disputes** **Probability Rating: 5 Impact Rating: 4**

This disruptive threat is the withdrawal of labor. It can follow a dispute between the workers and the Management of a company that has not been resolved. A withdrawal of labor is often accompanied by picketing across the entrance of the Company's premises to try to discourage anyone from entering. This sort of action is highly disruptive to the business and typically results in a shutdown until the dispute is resolved.

Loss of Utilities & Services

- **Power (elec.) failure Probability Rating: 4 Impact Rating: 3**

All organizations depend on electrical power to continue normal operations. Without power, the organization's computers, lights, telephones, and other communication media will not be operational, and the impact on normal business operations can be devastating. All organizations should be prepared for a possible electrical power failure, as the impact can be severe. Data can be lost, customers can be lost, and there can be a serious impact on revenue. Pre-planning is essential as a regional outage can cause a shortage of backup electrical generators. Consideration should be given to installing UPS systems to avoid brownouts.

- **Communications breakdown Probability Rating: 4 Impact Rating: 3**

Most businesses fully depend upon their telecommunications services to operate their normal business processes and enable their networks to function. A disruption to telecommunications services can result in a business losing revenue and customers. The use of cell-based telephones can help to alleviate this, but the primary reliance is likely to be on land-based lines.

- **IT system failure Probability Rating: 4 Impact Rating: 3**

With almost total dependence on IT systems within the vast majority of businesses, a failure of these systems can be particularly devastating. The types of threats to computer systems vary, including hardware failure, damage to cables, water leaks, and fires, air conditioning system failures, network failures, application system failures, telecommunications equipment failures, etc.

Other Emergency Situations

- **Mergers and acquisitions Probability Rating: 3 Impact Rating: 4**

Mergers and acquisitions can be extremely destabilizing for the employees of both businesses involved. Employees may be uncertain about how they will be affected or even whether they are about to lose their jobs. Unless well managed, the effect on the staff could be considerable, dramatically lowering morale and productivity.

- **Negative publicity Probability Rating: 4 Impact Rating: 4**

Unfavorable press comments can result in a lowering of employee morale or a loss of customers. Any company can suffer from negative publicity, and an internal crisis is best resolved from within before the media feeds the uncertainties and disputes. Reports may also be inaccurate, mainly where reliable information is not available, and therefore, well-worded press statements may be issued to quiet down adverse reports. Information can be leaked to the press from disgruntled employees and industry competitors.

- **Legal problems Probability Rating: 4 Impact Rating: 4**

Legal problems are both time-consuming and expensive. Organizations can experience various legal issues, including sexual harassment, contract disputes, copyright disputes, health and safety regulations,

and discrimination. Organizations must be fully aware of their legal duties and the rights of their employees.

1.05 KEY BUSINESS PROCESSES

The following is a descriptive list of CIM SECURITIES' key business areas. The list is in no particular order of importance to CIM SECURITIES. Each item includes a brief description of the business process and main dependencies on systems, communications, personnel, and information/data.

- **Counterparties**

Currently, CIM SECURITIES clears through the following counterparties:

Counterparty	Officer	Phone	Email	Address
N/A				

CIM SECURITIES has confirmed that in case of significant business disruptions at the above counterparties, their emergency standby system will fail after approximately 10 minutes. CIM SECURITIES will then be able to log into omnibus accounts. If the above counterparties' web access is available, counterparties will post on their respective websites that CIM SECURITIES may access its accounts via the web or desktop application or via telephone.

If an internal or external disaster causes the loss of CIM SECURITIES' paper records, counterparties will physically recover them from their backup site. If counterparties' primary sites are inoperable, counterparties will continue operations from their backup site or an alternate location. For the loss of electronic records, counterparties will either physically recover the storage media or electronically recover data from the backup site. If the counterparties' primary site is inoperable, continue operations from its backup site or an alternate location.

For further details about counterparties' disaster recovery plans, please refer to their respective copy of their Business Continuity & Disaster Recovery Plan held at our office at BD Main and backup copies in Willow, AK.

- **E-commerce processes**

a. STOCKS/ETFS Accounts: All client trading activity is primarily processed through an online platform that maintains all trading history, margin, equity available, etc.

b. Payments: The Company maintains all client payment processing through an online platform supported by the off-site firm.

- **Email based communications**

a. Internal Communication: Primary internal communication regarding the circulation of company documents.

b. Client Communication: Primary communication for trading hours, password, and account status notifications.

c. Vendor Communication: Office supply ordering, Invoice transmission, and account status notification.

- **Customer service handling**

a. Information requests, opening new accounts, transferring client funds, and giving global payment quotes.

- **Marketing, Sales, and public relations**

a. Brochures: Company literature regarding foreign exchange market and other financial products, managed account services, Payments, hedging services, etc.

b. Investor Newsletter: a monthly newsletter or other public dissemination to the customers or general public regarding CIM SECURITIES' products, services, performance in its managed accounts, and any new services being provided by CIM SECURITIES.

- **Information technology services**

a. They are maintained by Office Building, specifically by Office Suite Group (office space provider).

- **Premises (Head Office and branches)**

a. Head Office **(Tract B, ASLS 77-149, PLAT 79-3, Palmer, AK. 99645, Phone: 732-966-9244)** maintains all corporate documents, including all corporate financial & treasury documents, client information, etc.

b. The primary location of business or Head Office where all calls are directed

c. The back office is maintained in Willow, AK**.**

- **Accounting and Reporting**

a. Accounting is performed by outside accredited accounting firm, Goldman & Company, CPAs, which maintains its files regarding CIM SECURITIES' annual audit and other supporting documents.

b. Daily accounting and monthly reconciliation performed at the CIM SECURITIES' Head Office under the supervision of the Chief Executive Officer or Chief Financial Officer.

c. An annual audit will be conducted by Goldman & Company, CPAs.

- **Strategic and business planning activities**

a. Strategic and business planning activities include new market entries, mergers & acquisitions, and new product development.

b. For each significant essential business process, it is necessary to assess the financial and operational impact of disruption to normal business operations. A complete matrix analysis is shown below for each significant business process, ticking each box where a *"significant impact"* is likely.

	< 2 HOURS	2-24 HOURS	24 - 48 HOURS	2-5 DAYS	> 5 DAYS
BUSINESS PROCESS: E-Commerce					
Impact on Customer Services	X				
Loss of Customers	X				
Loss of Revenue	X				
Potential Additional Costs of Recovery	X				
Exposure to Penalty Clauses		X			
Exposure to Possible Litigation		X			
Loss of Key Information	X				
Negative Financial Impact	X				

	< 2 HOURS	2-24 HOURS	24 - 48 HOURS	2-5 DAYS	> 5 DAYS
BUSINESS PROCESS: IT					
Impact on Customer Services	X				
Loss of Customers	X				
Loss of Revenue	X				
Potential Additional Costs of Recovery	X				
Exposure to Penalty Clauses		X			
Exposure to Possible Litigation		X			
Loss of Key Information	X				
Negative Financial Impact	X				

	< 2 HOURS	2-24 HOURS	24 - 48 HOURS	2-5 DAYS	> 5 DAYS
BUSINESS PROCESS: Back Office					
Impact on Customer Services	X				
Loss of Customers	X				
Loss of Revenue	X				
Potential Additional Costs of Recovery	X				
Exposure to Penalty Clauses		X			
Exposure to Possible Litigation		X			
Loss of Key Information	X				
Negative Financial Impact	X				

1.06 IT AND COMMUNICATION

The disruption to and availability of IT services and communications is of particular importance when considering business risks and the impact of potential emergencies. The level of dependency that CIM SECURITIES has on IT and communications systems and the nature of customer services which are often on a 24/7 basis, has meant that it is essential that CIM SECURITIES be able to keep its IT networks and

communications systems operational at all times. This section examines some of the issues to consider when assessing the risk level associated with IT services and communications.

The following list includes the computer equipment currently in use by CIM SECURITIES and their description for replacement purposes:

Type	Model #	No.	Processors	RAM	Disks per terminal	Vendor	OS	Version	Users
Servers	N/A								
Workstation									

A digital backup of all data is stored at an off-site locations including Barracuda, Smarsh, OneDrive and DropBox. A copy of all the original system programs is stored off-site as well. CIM SECURITIES has included IT services that Office Suite Group maintains in its lease agreement.

Chief Financial Officer and Compliance department maintains all other financial information regarding bank account statements and client deposit history.

Emergency IT Contact Information (Office Suite Group):

Name	Title	Phone	Email	Address
Bryan Emerson	CEO, CCO, FinOp	907 795 5586	bemerson@cimsecurities.co	PO Box 810, Willow, AK. 99688

In the future, with the growth of the business, CIM SECURITIES plans the following:

A daily backup of all data is taken to tape and stored in the safe. Weekly, one tape containing a copy of all the data is stored at an off-site location. The system administrator reviews the system logs daily to ensure that the backup process has been executed successfully. Periodically the recovery process is tested to ensure that the recovery procedures are operational and valid.

A copy of all the original system programs is stored on-site in the IT library, and a further copy is stored off-site. A monthly backup copy of the system programs is made to ensure that all relevant software patches are included in the recovery processes. This monthly backup copy is also periodically tested to ensure that the recovery process is valid.

The servers used by CIM SECURITIES are also to be maintained by Level (3) Communications at a collocation. Services provided by Level (3) include the following:

Key Attributes

- State-of-the-art and secure
- Carrier-neutral
- Well connected
- Broad coverage
- Customized & pre-configured options

State-of-the-Art and Secure

- **Security**: Multi-layer security control procedures, biometric palm readers, and closed-circuit video monitoring
- **Power**: Uninterruptible AC and DC power solutions that are flexible and upgradeable — meeting all types of customer needs
- **Cooling**: HVAC redundant design with under-floor air distribution for maximum temperature control
- **Fire Suppression**: Smoke detection system above and below the raised floor; double-interlock, pre-action, dry-pipe fire suppression

1.07 KEY PERSONNEL CONTACT INFORMATION

Name	Position	Office	Mobile	Email
Bryan Emerson	CEO, CCO, FinOp	Head Off.	907 795 5586	bemerson@cimsecurities.com

1.08 KEY SUPPLIERS' & VENDORS' CONTACT INFORMATION

Name	Description	Contact	Main Number	Email	Fax
Abe Garcia	IT	TrifectaIT	619-760-0123	help@trifectait.com	

1.09 BUSINESS RECOVERY ACTIVITIES

Step 1:

A designated manager must contact all key personnel and provide the following information:

1) A meeting point if space has been damaged or a disaster prevents access to office space.

Step 2:

A meeting of executive managers can occur either in person or via a communication system (depending on availability) to determine the seriousness of the damages.

Step 3:

The executive managers may follow the plan described below for each situation that is most probable to occur after an assessment performed by the planning committee.

The following plans are to be followed depending on the disaster and its magnitude:

2) Disasters that hinder travel to work (Flood, Snowstorm, Freezing Conditions):

a) All key personnel have access to communications and computer equipment that will allow them to perform most of the key functions of the business.

3) Disasters that cause serious damage to operating equipment (Electrical Storms, Fire, Theft, Arson, Communication system failure.

a) Computer system: Vendors are to be contacted immediately for new equipment purchases. All data has been saved on the server located off-site. No data loss will occur.

b) Communication system: Additional phones are located off-site, which can replace the communication equipment until the features phone system can be replaced.

4) Disasters that cause serious damage and loss of data (Act of Sabotage, IT system failure)

a) Trading Information:

b) Client Information

c) Corporate Documents

d) Financial & Treasury Information:

All data is stored in the off-site server, which can be quickly restored. If an IT system fails, the collocation is maintained by its own personal generators. The system is also safeguarded against any acts of sabotage. Biometric palm readers and closed-circuit video monitoring restrict access to the server.

5) Disasters that cause severe loss to key personnel (Acts of Terrorism, Epidemic)

a) Key personnel includes all founding members of CIM SECURITIES. Each member is familiar with the tasks performed by the key personnel. Initially, the founding members will be responsible for taking over the functions of the key person lost. New personnel will then be trained in the everyday duties of the position. There is no continuity plan for the event that all founding members are lost to a horrific disaster.

2.0 BUSINESS IMPACT ANALYSIS (Key examples)

RISK EVENT	OFFICE BUILDING LOSS
PROBABILITY	Low
IMPACT	High
LIKELY SCENARIO	Fire, bomb threat, natural disaster
FUNCTIONS AFFECTED	All
ACTION	• Advise all business counterparties that are affected. • Move key staff and senior executives with phone or network access. • Call first responders and build security.
RESPONSIBILITIES	Senior Management at Site.
MITIGATION	n/a
CONSTRAINTS	The Company's general emergency procedures override these instructions if conflicts arise.
RESOURCES	Location of emergency phone: Location of the backup laptop: Location of roaming device:

RISK EVENT	LARGE ELECTRONIC DOCUMENTS LOSS
PROBABILITY	Low
IMPACT	High
LIKELY SCENARIO	Network problem (including cyber-attack)
FUNCTIONS AFFECTED	All electronic and paper-based document related activities
ACTION	**Immediately**: • Contact Help Desk [ph.] to log problem. • Contact IT Department [ph] to ensure problem is urgent. • Advise CTO [ph]. • Advise all affected business units.
RESPONSIBILITIES	Senior Management at Site.
MITIGATION	IT/Back Up, recover paper documents which are scanned to CD and copies held by back up business units.
CONSTRAINTS	It can take time to organize a recovery and to address cyber-attack.
RESOURCES	IT/Back Up (e.g. Third Party), CDs, Paper Documents.

RISK EVENT	SPECIFIC ELECTRONIC DOCUMENTS LOSS
PROBABILITY	Low
IMPACT	Medium to High
LIKELY SCENARIO	Documents accidentally deleted, cyber-attack
FUNCTIONS AFFECTED	All electronic and paper-based document related activities
ACTION	**Immediately**: • Contact Help Desk [ph.] to log problem. • Contact IT Department [ph] to ensure problem is urgent. • Advise CTO [ph]. • Advise all affected business units.
RESPONSIBILITIES	Senior Management at Site.
MITIGATION	IT/Back Up, recover paper documents which are scanned to CD and copies held by back up business units.
CONSTRAINTS	It can take time to organize a recovery and to address cyber-attack.
RESOURCES	IT/Back Up (e.g. third party), CDs, Paper Documents.

RISK EVENT	LARGE HARD COPY OR PAPER DOCUMENTS LOSS
PROBABILITY	Low
IMPACT	High
LIKELY SCENARIO	Fire, natural disaster, building loss
FUNCTIONS AFFECTED	File and document retrievals; all document-based activities
ACTION	**Immediately**: • Advise CEO and CCO. • Advise all affected business units for short and long term implications.
RESPONSIBILITIES	Senior Management at Site.
MITIGATION	Some documents e.g. Customer Contracts are scanned to CD, and copies are held by business units and online remote back up.
CONSTRAINTS	It can take time to organize a recovery of loss paper documents.
RESOURCES	IT/Back Up (e.g. Third Party), CDs, online back up.

RISK EVENT	SPECIFIC HARD COPY OR PAPER DOCUMENTS LOSS
PROBABILITY	Medium
IMPACT	Medium to High
LIKELY SCENARIO	Urgent - legal or regulatory requirements
FUNCTIONS AFFECTED	File and document retrievals; all document-based activities
ACTION	**Immediately**: • Check XXXX for possible locations. • Ask last known person involved with document. • Ask business unit – most lost documents are elsewhere in the requestor's business unit. • Check with Document Coordinators at likely sites • Put notice on staff bulletin board/broadcast email • Contact individual staff members who may have knowledge of the documents concerned. • If document is irrevocably lost, discuss impact with stakeholders, issue statement of search and loss signed by Document Manager.
RESPONSIBILITIES	Senior Management at Site.
MITIGATION	Some documents e.g. Customer Contracts are scanned to CD, and copies are held by business units and online remote back up.
CONSTRAINTS	It can take time to organize a recovery of loss paper documents.
RESOURCES	IT/Back Up (e.g. Third Party), CDs, online back up.

RISK EVENT	EMAIL & NETWORK DOWN
PROBABILITY	Medium
IMPACT	High
LIKELY SCENARIO	A malfunction in the computer system or on the LAN
FUNCTIONS AFFECTED	Business units requesting files and boxes (excludes interruptions to the file tracking software and database, for which see Software - XXXX System Down
ACTION	**Immediately**: • Contact Business Units by phone and ask that all communications be by phone, on paper or in person • Record all file requests on paper • When the system is available again, arrange data entry of all movements recorded on paper
RESPONSIBILITIES	Senior Management at Site.
MITIGATION	
CONSTRAINTS	
RESOURCES	Phone/Files/Forms.

RISK EVENT	FIRE OR WATER DAMAGE TO DOCUMENTS
PROBABILITY	Low
IMPACT	Medium
LIKELY SCENARIO	False alarm setting off sprinklers; or fire damage plus water damage from sprinklers and hoses; or storm water damage. Water damage is usually the most serious outcome of a fire.
FUNCTIONS AFFECTED	Business units requesting and using files.
ACTION	**Immediately**: • Put poly-tarps over affected shelves • URGENT: Assess damage (may require input from business units) – if more than is manageable in house, contact plumbing, cleaning and similar service providers to get quotes on removal, drying and cleaning. • Drying should begin within 24 hours to minimize damage. • Advise all business units of extent of problem and likely delays
RESPONSIBILITIES	Senior Management at Site.
MITIGATION	
CONSTRAINTS	• Poly-tarps only useful if water is in limited area. • Cost for use of commercial recovery specialists.
RESOURCES	Poly-tarps/email/phone.

RISK EVENT	ELEVATOR/LIFTS UNAVAILABLE
PROBABILITY	Low
IMPACT	Low for short duration, high for long duration
LIKELY SCENARIO	All lifts/elevators out of action due to mechanical fault; or some lifts/elevators out plus overcrowding and queueing at peak hours.
FUNCTIONS AFFECTED	File and box pickups and deliveries, mail handling clearance runs. Business units requesting and using files.
ACTION	**Immediately**: • Inform building maintenance. • Urgently needed individual documents can be faxed, or scanned and emailed to business units.
RESPONSIBILITIES	Senior Management at Site if problem escalates.
MITIGATION	• Be aware of peak load times for lifts, liaise with Property so we know of any planned significant outages • Fax and email services and scanning equipment available
CONSTRAINTS	The Company's general emergency procedures override these instructions if there are any conflicts
RESOURCES	Phone, fax, scanner, email.

RISK EVENT	PHONE SYSTEM UNAVAILABLE
PROBABILITY	Low
IMPACT	Medium
LIKELY SCENARIO	Phone system or phone line problems.
FUNCTIONS AFFECTED	• Business units requesting advice and files. • Contacting counterparties, key vendors.
ACTION	**Immediately**: • Contact all Business Units and suppliers by email or mobile phone and ask that all communications be by email or mobile phone.
RESPONSIBILITIES	Senior Management at Site if problem escalates.
MITIGATION	Mobile, email.
CONSTRAINTS	
RESOURCES	Email/mobile phone.

RISK EVENT	POWER OUTAGE
PROBABILITY	Low
IMPACT	High
LIKELY SCENARIO	Total power failure or power outage at specific power points.
FUNCTIONS AFFECTED	The main impact on all business units is if the outage is extended.
ACTION	**Immediately**: • A total power outage means no lifts, lights, phones, or computers. This will be managed by Company's general procedures and building safety guidelines. • Find out the extent and likely duration of the problem – contact [insert name] on [insert phone] if there are no broadcasts. • Use rechargeable flashlights.
RESPONSIBILITIES	Senior Management at the Site if the problem escalates.
MITIGATION	Follow standards & general emergency procedures.
CONSTRAINTS	The Company's general emergency procedures and building safety guidelines override these instructions if there are any conflicts.
RESOURCES	Mobile phones, rechargeable flashlights

RISK EVENT	TRADING SOFTWARE –SYSTEM DOWN
PROBABILITY	Low
IMPACT	High
LIKELY SCENARIO	The network is having problems, or the database is corrupted and being restored or rebuilt or issues on the server side.
FUNCTIONS AFFECTED	Customers, business units including back office, compliance, and finance.
ACTION	**Immediately**: • Contact IT and/or software vendor • Advise business units – compliance, finance, operations.
RESPONSIBILITIES	Senior Management at the site if the problem escalates.
MITIGATION	IT/Third-party backups.
CONSTRAINTS	Email/phone, only IT staff can identify if the problem is software or hardware related.
RESOURCES	Email, phone, paper.