SUGGESTED INCIDENT MANAGEMENT CHECKLIST

1. Planned response:

1.1 In the event of an enhanced threat ensure all plans are up to-date, with particular emphasis on:

- ✔ Updating all critical internal and external contact lists. Include the following information where it applies:
  - Home address
  - Home telephone
  - Mobile phone
  - Pager
  - Personal Digital Assistants (PDAs).
  - E-mail address

1.2 Consider the following:

- ✔ Establish a conference bridge. Provide all incident management team members with the conference bridge number and pass code.
- ✔ Establish a voice mailbox for employees to monitor for status updates.
- ✔ Determine if you should place third party business continuity and disaster recovery service providers on alert if you are a subscriber.
- ✔ Ensure that monitoring service vendors (e.g., Alarm Company) have current contact information.
- ✔ Identify a crisis command centre outside of the anticipated impact area.

2. Incident detection and preliminary assessment:

- ✔ Follow company emergency response procedures.
- ✔ Conduct a preliminary damage assessment, if it can be done safely. No recovery activities should be undertaken if personnel are placed in danger – liaise with Emergency Services.
- ✔ Scene may remain ‘Scene of Crime’ (police may need quite some time to gather evidence).
- ✔ Arrange for security of site once police hand site over. Security may be required to ensure sensitive documents, equipment and other items are not removed.
- ✔ Notify the incident manager and provide a detailed report.

- ✔ Activate incident management team:
  - The incident manager will determine if the incident management team should be activated and if necessary:
  - Open and commence log of events/decisions.
3. Notify Incident Management Team Members:

- Provide a description of the event
- Request that they assemble at the crisis command centre or participate via a conference call.
- Activate the crisis command centre.

4. Evaluate disaster impact:

4.1 Determine if the severity of the impact requires implementation of the recovery Plan.
4.2 Determine recovery objectives and activate recovery plan if necessary.
4.3 Notify recovery team leaders and members (see personnel notification guidelines below).
4.4 Brief recovery team leaders and alternates regarding:

- Priorities
- Strategies
- Action plans
- Assignments
- Timelines

4.5 Reporting and communications procedures:

- Declare a disaster with your third party business continuity and disaster recovery service provider if you are a subscriber.

5. Audit:

5.1 Consult/provide advice on changes to standard operating procedures to be implemented during the recovery effort.
5.2 Ensure that the following policies and standards are maintained during the recovery effort:

- Financial security and control policies
- Anti-fraud policies
- Information security standards.
- Provide reports and recommendations to the IMT as required.
- Provide additional resources to other business units during the recovery effort as needed.

6. Corporate Communications:

- Establish a media-briefing centre.
- Co-ordinate all media communications.
- Review and approve all statements regarding the incident.
✓ Develop both internal and external communications.
✓ Co-ordinate recovery related advertising with external vendors.
✓ Instruct employees to direct all media inquiries to corporate communications.
✓ Advise unaffected groups to prepare for accommodation sharing/relocating.

7. Environmental and safety:

✓ Ensure the health and safety of employees.
✓ Ensure that response activities to address fire, spills and/or medical emergencies are performed in accordance with regulatory guidelines.
✓ Notify regulatory agencies of the incident as required.
✓ Enlist the assistance of vendors and agencies to assist in support activities as appropriate.

8. Facilities:

✓ Conduct detailed damage assessment.
✓ Conduct salvage and restoration activities.
✓ Acquire replacement office space if necessary.
✓ Notify tenants of the incident and provide periodic updates regarding the condition of their affected office space.

9. Finance:

✓ Ensure funds are available for recovery.
✓ Ensure that all recovery expenditures are properly documented.
✓ Set up a recovery cost centre.
✓ Estimate the impact of the incident on the company’s financial statement.

10. Food Services:

✓ Provide foods services to recovery personnel at the alternate operating locations.

11. Human resources:

✓ Account for all personnel Complete and submit HSE Reports as required.
✓ Assist public authorities in handling casualties (i.e., identification of victims, family notifications, etc.)
✓ Monitor the condition and location of the injured.
✓ Co-ordinate employee communications with corporate communications.
✓ Co-ordinate additional or temporary staffing for recovery effort.
✓ Provide counselling services as required.
✓ Administer company personnel policies as they apply to response and recovery.
✓ File Worker’s Compensation claims.
✓ Assist employees with incident related benefit administration.

12. Insurance:

✓ Co-ordinate with insurance broker on the preparation and filing of all insurance claims.
✓ Document proof of losses.
✓ Submit claims and monitor payments.
✓ Establish a debris management programme.
✓ Involve Loss Adjusters.

13. Information technology:

✓ Conduct computer system and telecommunications damage assessment
✓ Activate alternate operating locations (for system recovery)
✓ Recover computer systems and network environment(s)
✓ Acquire and install replacement desktop computer equipment
✓ Re-establish data network connections to external resources (branch locations, vendors)
✓ Implement all telephone response plans (re-routing critical telephone numbers)
✓ Arrange for all alternate site telephone installations
✓ Ensure all system security devices and procedures are in place.

14. Legal:

✓ Manage all required regulatory notifications.
✓ Provide legal counsel for response and recovery operations.
✓ Review and approve new contracts acquired as a result of the event, before implementation.

15. Offices services (mailroom, shipping/ receiving):

✓ Re-establish mail and shipping services.
✓ Re-direct all mail and parcel receipts to alternate operating locations.

16. Purchasing:

✓ Manage all incident related purchasing.
✓ Acquire office supplies, forms and equipment for affected business units.
✓ Implement any necessary short-term financial tracking controls, using designated cost centres.

17. Records management:
✓ Co-ordinate with information technology to ensure the recovery of the records management system.
✓ Co-ordinate with business units in retrieving all off site backup records.
✓ Lead records reclamtion and reconstruction efforts.

20. Security:

✓ Co-ordinate onsite security for affected facilities and all alternate-operating locations.
✓ Control access to affected facilities.
✓ Monitor equipment and records being removed from facilities.

21. Transportation:

✓ Provide local transportation during response and recovery activities as required.
✓ Provide travel arrangements and accommodations for employees travelling to remote recovery locations.

22. Track incident status and recovery progress:

22.1 Conduct periodic debriefing sessions with recovery teams to monitor progress and determine problem areas.
22.2 Reallocate and/or provide resources.

23. Personnel notification guidelines:

Once recovery has been officially activated alert all personnel. Employees may be out of office at the time of the disruption and you may have to contact them at home or elsewhere. It is, therefore, advisable to have some form of standard instructions, for informing, which will not alarm members of a family or friends in such instances.