版 別 變 更 記 錄：
Version Change Record

版次 Version	日期 Date	變 更 內 容 摘 要 Description of Change
A0	2009/12/03	1st Release
A0	2010/12/23	No change
A0	2011/12/23	No change
A0	2012/12/21	No change
A0	2013/12/20	No change
A0	2014/12/23	No change
A1	2015/10/26	1. The Chief Corporate Risk Management Officer (CRMO) joins the organization of risk management steering committee. 2. Add S-004 Advantech Security Policy. 3. Update the Production Transfer Plan from M-07-TA022 to M-07-TM033. 4. Add the definition of RTO & RPO on section 6
A1	2016/12/27	No change
A2	2017/12/26	1. Delete the Chief Corporate Risk Management Officer (CRMO) from the organization of risk management steering committee. 2. Change “Emergency Operation Center Location B” from Shin-Tien to Linkou Office.
A2	2018/12/27	No change
A3	2019/07/24	Update the Advantech IT Backup System

會審單位：
Review Board

核 准 Approved By	審 核 Reviewed By	製 訂 Prepared By	發行 Issue
Deryu Yin		*NJ Lin*	

發行單位及要求份數 Issued to / # of copies					
	To / 份 copy		To / 份 copy		
	To / 份 copy		To / 份 copy		
	To / 份 copy		To / 份 copy	備註(Remark)：	

1. Introduction

Interruptions in service can occur for numerous reasons and with various degrees of severity. The objective of the Business Continuity Plan is to minimize business interruption and take steps necessary to ensure business continuity.
This plan provides the framework for the management of business and operational risk in the performance of Advantech's activities to meet the requirements of good corporate governance and protect the interests of Advantech's stakeholders.

2. Project Initiation and Organization

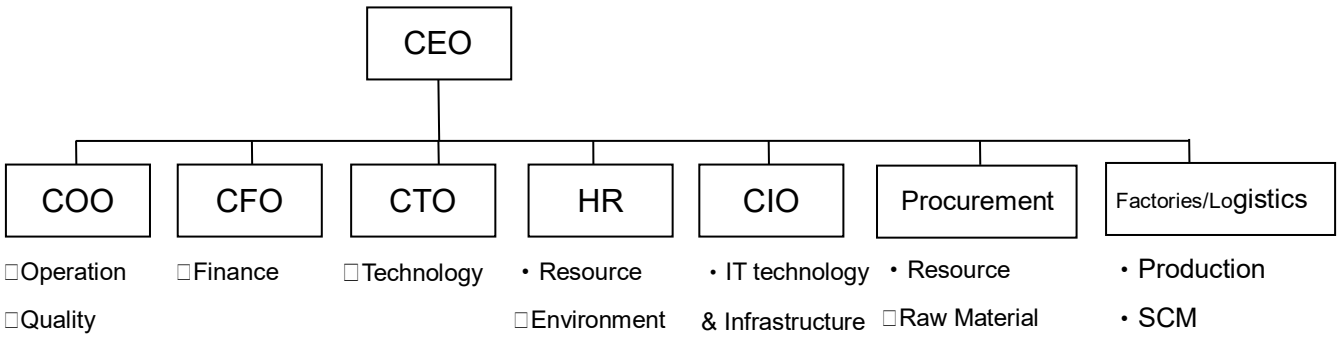
Role and Responsibility

Everyone in Advantech has responsibility for enterprise risk management. The Chief Executive Officer (CEO) is ultimately responsible and assumes ownership. The Management team supports the risk management policy & process, promote compliance with its risk appetite, and manage risks within their spheres of responsibility.

All employees are expected to be familiar with this policy, take a risk management approach to their work and escalate issues to the management team. The region, group and function heads are responsible for implementing the policy, monitoring its implementation in the everyday activities of their division.

The risk management organization consists of the key executives is required to review and monitoring of the risk management process to ensure that risks are effectively identified and assessed and that appropriate controls and responses are in place.

The organization of risk management



3. Risk Assessment

The Drivers of Key Risks

The risks facing an organization and its operations can result from factors both external and internal to the organization.

The following five key risk categories and five risk sources are identified:

Five Key risk categories:

- Financial Risks
- Operational Risks
- Technology Risks
- Quality Risks
- Human Resource Risks

Five risk sources:

- **Natural Hazard**: Significant geographical & natural environmental changes that pose impact or threat on Advantech's operation and business continuity.

- **Laws & Regulations**: Laws & regulations those are relevant to Advantech's operation ranging from labor insurance, health care insurance, and environmental regulations to accounting policies & financing regulation.
- **Misbehavior/Human Error**: Misconduct or human mistake/error of management, staff, first-line personnel that causes serious damage or loss of Advantech's operations and business.
- **Marco Environment:** Overall environmental factors that cause potential threat to Advantech's operations and business ranging from exchange rate, interest rate, political situation, important social event, educational level of invested area, significant market booming or depression that causes demand fluctuation, commodity and material price changes posing a threat to Advantech's operation and business, etc.
- **External Resource:** Resource outside the business scope of Advantech ranging from local community, financing resource (i.e. banks, bondholders, stockholders), government, suppliers, etc.

Risk Attribution by Departments	Risk Source									
	Natural Hazard		Laws & Regulations		Internal Resource		Macro Environment		External Resource	
	C1		C2		C3		C4		C5	
Technology Risk				Patent infringement／use of FOSS cause increased cost and failure to deliver products (Preventive: IPR management system,(i.e. patent mapping, patent portfolio) , all software used is purchased through ITD with legal contract with software company, ban of illegal software usage. Reactive: Patent right negotiation, Retain the legal lawtrace right of any employee that use illegal software.)		Information security system failure may cause ERP system & PLM system shutdown and delay ODM project progress. (Preventive: Firewall, antivirus software installation and execution, regular data backup, Reactive: data saving and re-storage, bug fixing plan)				
				New Capital adequacy regulation may cause higher threshold on equity.		Information system & MIS system failure				

Risk Attribution by Departments	Risk Source									
	Natural Hazard		Laws & Regulations		Internal Resource		Macro Environment		External Resource	
	A1		A2		A3		A4		A5	
Financial Risk		Earthquake, typhoon and flood cause fixed Asset Loss. (Preventive: Insurance coverage, equipment repair／rescue operation rehearsal, Reactive: equipment repair, rescue operation)		Change of law causes higher taxation cost				Demand fluctuations may cause uncertainty of fund raising		Higher cost due to the higher interest of alliance banks.
				Change of law may require higher financing threshold and increase the difficulty in fund raising.				Product pricing fluctuation may cause uncertainty of revenue and financial forecasting		Risk in funding due to the financial difficulty of alliance banks.
								Fluctuation of material prices may causes uncertainty of cost		Difficulty in fund raising due to low liquidity of stock market. (i.e. bear market)
								Fluctuation of Interest rate causes uncertainty of cost ／fund raising		
								Fluctuation of exchange rate causes uncertainty of cost		

Risk Attribution by Departments	Risk Source									
	Natural Hazard		Laws & Regulations		Internal Resource		Macro Environment		External Resource	
	E1		E2		E3		E4		E5	
Human Resource Risk		Infectious disease (e.g. SARS) spread out causes high employee absence rate		Labor laws and regulation change may cause higher labor cost.		R&D team members move to competitors forcing the ODM project on-hand halted. (Preventive: PLM data recording so that project is able to run w/o RD team, sign NDA contract with RD, Reactive: fill in newRD to run ODM project.)		Difficulty in recruiting due to relatively unattractive compensation level.		
								Employees strike may cause scheduling risk and delayed delivery		

Risk Attribution by Departments	Risk Source									
	Natural Hazard		Laws & Regulations		Internal Resource		Macro Environment		External Resource	
	B1		B2		B3		B4		B5	
Operational Risk		Earthquake, typhoon and flood cause factory shutdown (Preventive: production transfer plan, better construction design to resist stronger hazard, Reactive: production transfer plan execution)		Environmental laws and regulations may cause higher operation cost		Human error and misbehavior may cause fire in factory & warehouses		Demand decline causes increased inventory		First supplier source is not available due to natural hazard or other risk (Need second source vendor).
		Greenhouse effect causes higher operation cost		Engineering Security laws and regulations may cause higher operation cost		Misbehavior may cause power shutdown of factory and warehouses		Demand boost causes product ramp-ups and insufficient capacity. (Preventive: long-term demand forecasting, capacity buffer plan, Reactive: short-term outsourcing plan)		Product delivery delay due to the late EOL notification of sub-suppliers. (Preventive: provide material forecasting data so that sub-suppliers is able to prepare components in advance, second source approval)
				Regulation is not compliance with local safety requirement.				Customer application is over product Spec that may cause risk.		Unfriendly political environment to the intension between Taiwan and China
										Unfriendly community due to moral issues (i.e. environmental protection issue, labor abuse issue.)

Risk Attribution by Departments	Risk Source									
	Natural Hazard		Laws & Regulations		Internal Resource		Macro Environment		External Resource	
	D1		D2		D3		D4		D5	
Quality Risk						Poor design may cause product functions is not in compliance with design spec (Preventive: ensure Product concept & Product planning quality, capture customer requirement, Reactive: Gatekeeper of EVT & PVT phase may return design prototype until design is in compliance with spec and customer requirement)				
						Poor product safety may cause injury or loss of customers. (Preventive: NPI system ensure higher quality and product safety, product liability plan, Reactive: product recall plan)				

4. Business Impact Analysis and Risk Reduction Strategies

Advantech is managing its risk and implemented it into its daily operation. For example, fire drills are held in a regular basis to prevent operational risk; data maintenance of IT system is also a daily operation ensuring the mitigation of potential IT risk.

Since Advantech has identified the risk scenarios showed above. We are able to nominate proper risk owner and action owner to implement actions

Risk response of Advantech involves several standardized procedures and can be described in the risk flow chart below. The framework of risk response can be further separated into two elements and four strategies: prevention action plan & corrective plan and passive accept avoidance, mitigation & transfer, respectively. Risk" - Defines the vision, strategy, the process and the overall introduction of risk management system.

Building destroyed (including caused by Earthquake, Hurricane and Flood)

Damage to employees, departments, properties cannot be foreseen. In case the building is destroyed the normal governmental help, evacuation and escalation will be activated. As soon as possible health and care actions need to be taken for our employees and a status needs to be made up and communicated. The Resumption Management Team has to

decide and initiate actions to ensure business continuity.

Fire and/or Smoke

Fire can result in partial or total loss of printed data for an extended period. Recovery is slow or impossible.
The damage from smoke occurs much faster than damage from the actual fire or water.

In the building the Safety Instruction procedures are in place and the building is built to conform to the latest fire protection requirements. Fire doors are located between floors and escape routes are defined and published.

Staffs are aware of fire prevention and new hires are informed during induction training. Emergency members are appointed for the different floors/departments.
The current fire detection system consists of smoke detection units placed on the ceiling all over the building. Also the auto water spreading system is in place for all building. Server room has auto fire extinguisher system (HFC-23). And B1 control-monitoring room has dedicated person watch for the sensors (temperature, smoke, humidity, and door) at server room.

Hand operated fire extinguishers are in place. A fire prevention program is in place to inspect these systems. Employee training is completed to ensure quick application and safety of employees using the equipment.

Loss of Power

Loss of building power at the ACL building will have no effect on the servers etc because they are secured by UPS. The batteries of UPS are replaced every 2 years. As soon as power loss is detected a diesel generator will supply power to ensure that all datacom/networking including phones will be working. The diesel generator is tested every 3 months. Power of users' computer is also provided by the diesel generator.

System Contamination

Viruses or system contamination may take several forms, such as software worms, viruses, etc. Any one of these problems can render data useless or unrecoverable. Even more, the network traffic could be compromised by the spreading of viruses/worms. The IT organization provides users to have the proper anti-virus software and patches installed/updated via central anti-virus server and Windows SUS server.

All business essential applications and databases are backed up daily, and the data is copied to the remote site.

Hardware Failure

Mission critical applications such as ERP are protected by H.A. solution. There is also a dedicated network line connected to Milpitas office for ERP data synchronization. The ERP system backup site in Milpitas/USA will be enabled once the ERP system in HQ/Taipei has severe issues and cannot be recovered in a short time. Other servers also have RAID 5 or RAID 1 hard disk configuration to ensure the data protection. Air condition in server room is redundant. The IT network environment is organized in such a way that all HW and lines (intranet and internet) are backed up so that if an individual unit is down the network can continue to operate.

IT Disaster

The management of an IT location must concern itself with safeguarding the resources under its control. Part of the IT management task is to protect the information resources and also to safeguard operating system, operating software, database information and documentation that are essential to re-establishing the environment in the event of a disaster.
The Disaster Recovery Plan (DRP) establishes a common format for action and provides the framework within which each IT location defines procedures for designed individuals to react to an interruption of services. The plan will contain specific detail information for the location
The purpose of **Advantech IT Disaster Recovery Plan** is to provide for the continuation of Data Processing services for users located at any site of Advantech in the event of total destruction or temporary disablement of all or any of the IT Managed Services.
(also refer to: C-005 Advantech IT Disaster Recovery Plan)

Employee Sabotage

Physical damage to company data or facilities by disgruntled employee(s) can pose a serious threat to data integrity. An effective guideline for the handling of human relations issues will minimize the exposure to these risks.
Advantech uses password protection to control access to all essential applications. Facility access is controlled by manual card identification. A checklist used during the employee termination process insures that all access codes and passwords are disabled.
(also refer to: S-004 Advantech Security Policy)

Intrusion of Unauthorized Personnel

Secure facilities and thorough data backup and protection minimize the loss associated with these types of threats.
Facility access is controlled by manual card identification. All visitors are required to sign a visitor book and require escort by an Advantech employee.

Influenza pandemic

In the event of any influenza pandemic, employers will play a key role in protecting employees' health and safety as well as in limiting the impact on the economy and society. Employers will likely experience employee absences, changes in patterns of commerce and interrupted supply and delivery schedules.

Proper planning will allow employers to better protect their employees and lessen the impact of a pandemic on society and the economy. The plan includes the following components:

- ✓ Employee Education (personal hygiene) and Work Environment
- ✓ Measures to protect employees and corresponding actions to ensure that business operations can continue.
- ✓ Policies for flexible sick leave, flexible worksites to promote social distancing if flu conditions become more severe.
- ✓ Identified essential business functions and critical supply chains (e.g. raw materials, suppliers, sub-contractor services/products, and logistics) that are needed to keep our business running.
- ✓ Triggers and procedures for activating and terminating the pandemic plan.
- ✓ A process to communicate information to employees and business partners on the pandemic plan.

(also refer to: E-08-A001 Pandemic Planning)

Dual-Manufacturing center concept

Though not systematically implemented, the business continuity and contingency plan is always part of Advantech's daily operation and will be further become a fully integrated system. Now, Advantech has two major manufacturing sites in Taiwan and China. It is the so called "**Dual-Manufacturing center concept**". It is to prevent uncertainty risk and hazard risk damage Advantech and customer's business operation, we have developed an integral line transfer plan. Given any one of our factories being destroyed, Advantech is still able to transfer production line to another factory. Advantech Emergency Response Policy is designed for unexpected calamity over our manufacturing premises including **preventive plans** before accident and **action plans** after accident**. Production Transfer Plan (M-07-TM033)** describes how to **transfer the capacity and production line** effectively in four months.

(a) Material & inventory

Material and inventory is managed by Advantech's SAP ERP System. Thus, we have full documentation & record to help Advantech keep track of material and inventory. With the information, Advantech is able to acquire the components or inform sub-suppliers to provide it for the production line.

(b) Personnel

Advantech has assigned tasks / responsibilities to the counterparts for both manufacturing sites. Given the situation that personnel in one of the manufacturing site is unable to transfer to the other plant (i.e. injuries or dead) , Advantech is ready to assign their tasks to the personnel of the functioning site. If the personnel is able to transfer to the other plant, Advantech also has proper plan to transport personnel

(c) Information & IT system

Advantech is using SAP as its ERP / MRP system for both sites. Data maintenance is a daily operation to ensure that data contained therein is backuped.

Advantech Backup System

Targets: ACL critical data that need to be backed up on daily basis. Includes ERP (SAP), Mail (Exchange 2013 & Office 365), PLM (Agile), CRM (Siebel), B2B, FTP, and file server.

Backup Software: ACL is using Veeam backup software to backup its critical data. This backup software is installed in a dedicated computer to perform the data backup and management tasks.

(SAP data is backup by HP Data Protector System)
Backup schema: D → D → T (Disk to Disk to Tape)
Backup schedule: Data is fully backed up once per week, and incremental backup is performed in the rest of week.
(SAP clones 2 full copies of ERP DB to the clone disks per day)
Tape Library: SAP uses HP MSL-5030 LTO Library (30 slots)
Daily Check: ITD is responsible for daily backup status check. Any unsuccessful backup task will be escalated to IT manager.

(d) Dual Supplier Qualification

Advantech is now double recognizing the sub-suppliers for both sites (Taiwan & China) to ensure that material & components supply network remains functional give one of the manufacturing sites being destroyed.

Procurement BCM

Second-source policy

Based on

- Cost advantage
- Mat'l supply flexibility

- MFG site
- Customer requirement

In order to well control the parts, Advantech has summary report to define second source policy base on design and manufacture.

Definition of suppliers' roles and responsibilities

Advantech has detailed defined suppliers' roles and responsibilities in Advantech Supplier Survey Form, including suppliers' management for environment, health and safety etc.

5. Disaster Recovery Planning and Testing

Resumption Management Team

Overall Responsibilities

Is responsible to manage all aspects of the disaster response including evacuation, recovery, and relocation.

1. Confirms the disaster, contacts and coordinates support.
2. Confirms availability of Emergency Operation Center location and initiates Disaster Communication plan.
3. Coordinates all other teams and is responsible of obtaining any resources that may be required by them to meet their objectives.
4. Maintains communication with Advantech Management.
5. Supervises the business resumption plan test.

Pre-Disaster Duties

1. Identify team leaders for all disaster recovery teams.
2. Develop guidelines for the Emergency Operation Center that will be used as a focal point for the dissemination of information in the event of a disaster.
3. Develop criteria for system back-up site selection.
4. Ensure that team members for all teams are confirmed, and their respective responsibilities are known.
5. Develop a plan to test the Disaster Recovery Plan.

Post-Disaster Duties

1. Confirm disaster.
2. Contact Resumption team and disaster recovery teams.
3. Assemble all team leaders at a convenient location.
4. Use the following agenda to conduct the initial meeting:
   Communicate known details of disaster.
   Visit site if possible.
   Review Disaster Plan and Team Responsibilities.
   Evaluate need for Emergency Operations Center.

Have managers identify critical processes scheduled for the next 5 days.
Script standard message to use when contacting customers.

5. Start Dot.com notification and prepare for local press notification. Make selection of Emergency Operation Center.
6. Activate the Emergency Operation Center.
7. Activate Disaster Communication Plan as documented in this guild.
8. Evaluate the extent of damage from Facility Team reports and Hardware and Documentation Salvage Team reports.
9. Determine whether the current ACL facility can be made 50% operational within 4 working days or if the operation should be moved to a backup service facility.
10. Activate appropriate teams, based upon the previous decision. Notify Administration Team to secure a backup service facility ASAP if the decision is to move to a backup service facility.
11. Monitor and coordinate all team activities as dictated by the type of disaster.
12. Provide directions or decisions for unexpected occurrences.
13. Handle public relations and press releases.
14. Handle unplanned financial decisions.
15. Prepare final report and recommendations.

Administration Team/HR

Overall Responsibilities

1. Provides administration support for all other teams pertaining to logistical, financial and human resource matters.
2. Disseminates information on current status of organization (internal only).
3. Establish a man power pool.

Pre-Disaster Duties

1. Verify annually that the proposed Emergency Operation Center locations are available for use in the event of a disaster.
2. Establish emergency supply requirements and store a temporary interim emergency supplies at a location that is accessible for the Emergency Operation Center location.
3. Negotiate and regularly review standby leasing provisions for short-term hardware procurement such as facsimile, photocopier, personal computers with corporate recommended software, laser printers, desk, chairs, lighting, filing cabinets, etc.
4. Define administration center procedures and functions to ensure rapid and effective dissemination of information to all teams.
5. Define essential administration functions; these definitions should be made available to all teams, to ensure that expectations are clearly set prior to a event of disaster.
6. Maintain Disaster Recovery Plan and Disaster Recovery Databases.
7. Define an introductory list of supplies to obtain for the Emergency Operation Center.

Post-Disaster Duties

1. Team Leader notification.
2. Upon Resumption Management Teams direction to activate the Disaster Communication Plan, all Advantech staff should be notified by using the Disaster Communications Plan as stated in this document and through the use of phones.
3. Staff availability is assessed for the purpose of staffing a manpower pool. If insufficient, seek additional support.
4. Administrative duties allocated.
5. Equip the Emergency Operation Center with required facilities and equipment.
6. Make available the Emergency Response Administrative Services and forms documentation, to all teams.
7. Put up notices at disaster site to inform staff of:
   - Emergency Operation Center
   - Key services provided, etc.
8. Communicate with other teams to meet specific requirements, such as mail delivery, transportation, etc.
9. Coordinate with the Facilities Team the purchase/lease of all needed supplies and office equipment.
10. Set-up a message center.
11. If the decision is to use a backup services facility, seek and negotiate possible use of one of the facilities documented in this guide.
12. Acquire services and support as required.

Facilities Restoration Team

Overall Responsibilities

1. Assists local authorities in securing the damaged facility.
2. Establish a methodology to quickly restore facility function and data processing capability at the original site or an alternate facility.
3. Coordinates with the Administration Team the purchase/lease of all furniture and facility support equipment which must be replaced both temporarily and permanently.
4. Coordinates and approves deliveries to original site.
5. Maintaining trained personnel for emergency response team (Fire Wardens).
6. Provides Resumption Management team with an initial report of facility damage.
7. Maintain disaster recovery plan and database.

Pre-Disaster Duties

1. Provide emergency response fire extinguisher training to employees as required.
2. Provide orientation on hazardous materials for Facilities team members.
3. Communicate with Administration Team to define notification process for them to initiate emergency procurement for items identified as unsalvageable.

Post-Disaster Duties

1. Team Leaders notify Alternate Team Leader.

2. Team Leaders notify team members.
3. Team members assist local authorities if possible in securing the damaged facility.
4. Team Leaders supply Resumption Management team with an initial report of facility damage.
5. Coordinate and approve deliveries to the original site.
6. Communicate with Hardware and Documentation Salvage Team to begin salvage operations after necessary approvals have been obtained by insurance companies.
7. Assist the Hardware and Documentation Team with restoration of recoverable furniture and office equipment.
8. Communicate with local vendor contractors for support on damaged office equipment (copiers, fax machines).
9. Coordinate the replacement of destroyed furniture and office equipment with Facilities, Hardware and Documentation Team and the Administration Team.
10. Move usable and restored furniture, or equipment to the back-up or original facility.
11. Assist local contractors when necessary with restoration of facility.

Technical Support/IT

Overall Responsibilities

1. Assists Hardware and Documentation Salvage team at disaster site until decision is made to establish operations at backup site.
2. Responsible for movement of tape media from the off-site storage location to the backup site, and prepares the host required to maintain the critical business applications.
3. Establish network and telecommunication connectivity, and provide hardware maintenance support at the backup site.
4. Assist the Administration Team in procuring all computer and telecommunications hardware and software, which must be replaced both temporarily and permanently.

Pre-Disaster Duties

1. Compile and store off-site: schematic drawings of all-in house LAN and telecommunication configurations, peripheral hardware, server descriptions and specifications, printers, and telephone interfaces.
2. Compile and store off-site, an inventory of all PC software by department for standalone PC and LAN installations.
3. Compile inventory of all PC hardware with serial numbers and store off-site.
4. Establish LAN standard and configuration standards and store off-site.
5. Update Operating Procedures to reflect the polices for installation of software, and recommended backup and security procedures for PCs.
6. Develop with telecommunications vendors, all requirements for recovery and call forwarding to occur in the event of a disaster.
7. Negotiate contractual agreements with appropriate off-site media storage facilities.
8. Develop a test plan and periodic test schedule for all information backups, to ensure

desired data is available and complete as expected in the event of a disaster (Technical Support Team provides).

9. Establish procedures for information security. This includes guidelines for handling employee turnover (i.e. changing access cards, etc.), secure access to information storage facilities, and password protection for all systems including personal computers.
10. Ensure safe storage of all operating procedures with respect to information storage. This information should be stored appropriately with respect to the level of exposure to risk, and proximity to area where needed.
11. Train team members to react quickly and perform the following tasks if reaming on site during initial stages of a disaster doesn't pose any danger to human lives.
    - Complete final backups of at risk information and complete orderly shutdown of LAN.
    - Assist Hardware and Documentation Salvage Team in shutting down and covering at-risk systems and data.

Post-Disaster Duties

1. Team Leader notifies Alternate Team Leader.
2. TL and ATL establish assembly time and location.
3. TL and ATL notify Team members.
4. Team meets, reviews responsibilities, assigns duties, and notify the Administration Team to procure any necessary tools to complete the required duties.
5. Team receives clearance from Facilities Restoration Team to enter building.
6. Assist Hardware and Documentation Team with inventory of all computer and telecommunications hardware, label as destroyed, recoverable, or useable.
7. Contact vendor support as necessary.
8. Restore network and telecommunications at the disaster site if decision is made to stay.
9. Restore network and telecommunications at the back-up site if decision is made to move.
10. Communicate equipment and vendor support needs to Administration Team, and coordinate equipment installation and set-up at the back-up site, and at the original site.

IT Disaster Recovery Plan

The Disaster Recovery Plan (DRP) establishes a common format for action and provides the framework within which each IT location defines procedures for designed individuals to react to an interruption of services. The plan will contain specific detail information for the location

The purpose of **Advantech IT Disaster Recovery Plan** is to provide for the continuation of Data Processing services for users located at any site of Advantech in the event of total destruction or temporary disablement of all or any of the IT Managed Services.

(also refer to: C-005 Advantech IT Disaster Recovery Plan)

Customers Services

Overall Responsibilities

1. Responsible for movement of support materials from the off-site storage, or disaster site, to the back-up site.
2. Provide customer service functions and operations from the back-up site until the disaster site is operational, or operates from the disaster site if it can be partially restored.

Pre-Disaster Duties

1. Develop a plan to designate responsibilities for completing all critical processes.
2. Maintain off-site inventory of all operating procedures, necessary forms, etc.
3. Establish a list of emergency supply requirements to be acquired upon notification, to establish operations at the back-up site.
4. Team periodically meets, gathers, and reviews responsibilities, procedural, and operational documentation from off-site storage.
5. Participate in disaster plan testing.

Post-Disaster Duties

1. Team Leader notifies Alternate Team Leader.
2. Assist Salvage teams as necessary until notification to resume partial operations at the disaster facility, or until notified to establish operations at the back-up facility.
3. Wait for notification from the Administration Team to begin operations from damaged facility or established back-up facility.
4. Upon notification, Alternate Team Leader notifies team members of assembly time and location.
5. Make arrangements to transport personnel, documentation from off-site storage and supplies to the back-up facility.
6. Team Leaders requests necessary supplies, equipment, and furniture from Administration Team.
7. Team Leader requests computer and telecommunications support from Technical Support Team.
8. Team members assist with set-up of operations site.
9. Establish customer operations.

Helpdesk/Communication

Overall Responsibilities

1. Responsible for reporting, resolution and follow-up of problems associated with services provided to our customers.
2. The Help Desk Team will provide a focal point for customers to interface with their Advantech business team as required.

Pre-Disaster Duties

1. Participate in disaster testing exercises, assisting other teams as needed.

Post-Disaster Duties

1. Team Leader notifies Alternate Team Leader.
2. Team Leaders confirm space availability at Emergency Operation Center location.
3. Team Leaders notify Help Desk team members.
4. With the assistance of the Resumption Management Team, script a message summarizing the disaster. This message will be communicated on a limited basis as requested by the Resumption Management Team to our customers and will ensure that a uniform message will be delivered to everyone.
5. Team meets, reviews responsibilities, and gathers customer lists and all needed supplies.
6. Coordinate telecommunications needs and call rerouting with the Technical support Team.
7. Receive and respond to rerouted phone calls from the disaster site.
8. Establish a status board.

Hardware and Documentation Salvage Team

Overall Responsibilities

1. Assess the extent of damage to computers and telecommunications equipment and accounting documentation files.
2. Minimize further losses, and coordinate salvage of hardware and documentation.
3. Provides Resumption management Team with reports of recoverable and non-recoverable materials.

Pre-Disaster Duties

1. Decide whether hard copy data is to be electronically replicated and incorporated into the backup process, or physically copied and moved to appropriate storage facilities and then carry out that decision.
2. Create forms for identifying items that are destroyed, recoverable, or usable.
3. Apprise Administration Team of initial purchases required in the event of a disaster.

Post-Disaster

1. Team Leader notifies Alternate Team Leader.
2. Team Leaders notify Team members.
3. Team meets, reviews responsibilities, assigns tasks, and notify Administration Team of tools, supplies and equipment required for recovery or salvage process.
4. Team receives clearance from Facilities Restoration Team to enter building.
5. Video tape all damage.
6. The team will make an assessment on the extent of damage and determine best course of action for salvage operations.
7. Develop salvage operation plan.
8. Coordinate effort to preserve site to prevent further loss of furniture, equipment, and documentation.
9. Coordinate effort to preserve and restore wet documentation by immediate drying or

freezing.
10. Inventory all furniture, equipment, and documentation.
11. Move furniture, equipment, and documentation to safe area for evaluation of loss.
12. Clean, inspect and test furniture, equipment and documentation as needed to prepare for re-deployment.
13. Determine usability of furniture, equipment and documentation.
14. Notify Tech Support of damaged computer equipment.
15. Notify Facilities of damaged office equipment and furniture.
16. Notify respective manager of damaged documentation.
17. Notify Facilities Restoration team of items available for re-deployment and use.
18. Determine the extent of loss using inventory listings.

Emergency Operation Center

In the event of a disaster which makes the Advantech Nei-Hu HQ inaccessible, or unusable, employees will be notified to report to work at the location designated as Emergency Operation Center Location A. If Emergency Operation Center Location A is not available, employee will be asked to report to Emergency Operation Center Location B.

Emergency Operation Center Location A
Advantech SUN-Building Office

Emergency Operation Center Location B
Advantech Linkou Office

The facilities available at the Emergency Operation Center Location should include:
1. Conference rooms capable of seating 20-40 people would be used for administrative purposes and small meetings. Each room requires a phone line.
2. Motel rooms will be acquired for administrative purposes or control centers as necessary.

Disaster Communications Plan

Employee Notification

When a disaster occurs, management will use the following method to provide information to employees:
1. The Resumption management Team will provide assembly instruction to the HR team or Disaster Recovery team who will phone all employees and inform them of the assembly plan.

Disaster Voice Telecommunication Options

In the event of a disaster to the ACL, the following options are available for telephone support:

1. PHS cell phone provided by Advantech will group all key members together, when a disaster occurred.
2. Calls to ACL can be re-routed to another number (Like Shin-Tien office) within one hour.

Post-Disaster Communications

The HR/Administration Team will establish, in the Emergency Operation Center, an action item board for each Disaster Recovery Team. This board will be used to list, and record completion of all team activities.

The Technical Support/IT will establish one phone number, as a Hot-Line, to be accessible only by Advantech management and Disaster Recovery Team Leaders.

Communications to BU/Countries.

Disaster Recovery Plan Testing

Testing the Plan

It is essential that the plan be thoroughly tested and evaluated on an annual basis. Procedures to test the plan should be developed and maintained.

The tests will:

1. ensure that all necessary steps are included in the plan;
2. determine the feasibility and compatibility of back up facilities and procedures;
3. identify areas in the plan that need modification;
4. provide training to team managers and team members;
5. demonstrate the ability to recover;
6. provide motivation for maintaining and updating the plan.

After a test plan has been completed, an initial test of the plan should be performed by conducting a structured walk-through test. There are different types of tests, such as checklist, simulation, parallel tests, and full interruption test. The test will provide additional information regarding any further steps that may need to be included, changes in procedures that are not effective, and other appropriate adjustments. The plan should be updated to correct any problems identified during the test.

6. RTO (Recovery time objective) and RPO (Recovery Point Objective) - Disaster Recovery Plans per discipline

Zero Processing Duration Assumption

This plan uses the assumption that the ACL productivity is reduced to “zero processing” for 3 days, would have a minimum impact to Advantech Corporation. Processing down time exceeding 3 days would become increasingly damaging to corporate operations. This assumption considers the possibility that a disaster could occur during the worst possible time period, during month-end or year-end closing operations.

Overview

Following is a possible sequence of events that could occur following a disaster impacting the ACL. The actual sequence or actions may be modified by the Resumption Management Team as conditions require.

1. Immediately following a disaster, the Resumption Management Team will meet, confirm the Emergency Operation Center site availability, and develop a briefing to provide situation information, disaster recovery information, and employee responsibility assignment information.
2. The Resumption management Team will notify the HR/Administration Team who will meet at a designated area to coordinate facility arrangements and communicate instructions to employees.
3. All teams activated by the Resumption Management Team will meet at the Emergency Operation Center to receive situation information, and an updated disaster recovery responsibility assignment. The employees will then receive further instructions from their Disaster Recovery team.
4. The Technical Support/IT Team will contact appropriate telecommunications vendors and make arrangements to re-route calls to the Help Desk Team/Communication point located at the Emergency Operation Center.
5. The Resumption Management Team will determine, on the first day following the disaster, whether the Advantech facility can be made 50% operational within 3 working days, or if operations will be moved to a back-up facility.
6. If it is determined that the Advantech facility can be restored to provide business essential functions to 50% or more of the current staff within 3 working days, then efforts will be directed to accomplish this goal.
7. If the decision is made to move operations to a back-up facility, then the appropriate teams will begin the necessary processes.
8. All team assignments and a brief functional description are provided in this document. Actual assignment and functions may be modified by the Resumption Management Team as conditions require.
9. At noon, each day following the disaster, the Resumption management Team will meet, or teleconference with each Recovery Team Leader to acquire situation updates, coordinate team activities, and develop recovery work-plans.
10. It is the responsibility of the Resumption Management Team to keep this document updated, and insure that a copy is always available off-site.