15

POLICIES AND PROCEDURES

Get Everyone Moving in the Same Direction

In the midst of chaos, there is also opportunity.

—SUN TZU

INTRODUCTION

A big challenge in getting an organization back up and running after a disaster can be its own employees. Their focus is typically on their own area or department, and they are not always aware of all the ways their work affects others in the organization. Their pay and promotions typically depend on optimizing their own area, so they don't always appreciate the big picture. Many people feel that their area or department is the most critical, but recovery of their area after a disaster may not be the highest priority for the organization.

Well-crafted policies and procedures can guide employees by explaining to them how to best support organizational recovery efforts. They provide direction to employees in situations that are not specifically covered in business continuity or disaster recovery plans.

This chapter addresses what you should include in your policies and procedures to support recovering the organization from a disaster. Your policy and procedures are not intended to replace instructions in your business continuity or disaster recovery plans, nor recovery instructions from your hardware and software vendors. The examples included in this chapter are meant to guide you in crafting your policies and procedures to your unique circumstances; there is no "one size fits all" solution.

POLICIES

Policies are general statements of direction that provide employees guidance in the shared goal of supporting the mission of the organization. Management cannot and should not have to make every decision during a recovery, as this would greatly slow down the process. Not every set of circumstances can be anticipated in advance, so employees need guidance on how to make appropriate decisions on their own. Policies do not specify exactly what should be done in a given situation, but rather provide objectives and boundaries to guide employees to make decisions in the best interest of the organization.

Well-written policies give employees the freedom to make decisions with the best information available at the time, which promotes ownership of the results. With proper guidance, employees who are closest to the work are in the best position to take the best course of action.

Policies explain the "what" and "why" for taking action in a given situation. They should never be used as a substitute for common sense and sound judgment. They should be written at a reading level that is appropriate for your workforce, and be clearly understood by anyone that may need to reference them in an emergency. Policies have the following characteristics:

- Present a high-level statement affecting a large part of the organization.
- Provide general guidance on the appropriate action.
- Change infrequently.
- Tell the "what" and/or "why."
- Address major operational issue(s).
- Define the goal to be achieved.

PROCEDURES

Procedures are specific instructions on how to perform an activity. They give detailed instructions on how to perform a well-defined function to achieve a particular result. Procedures are important when a series of tasks need to be performed precisely, with little or no room for deviation. They can be used as performance measures, as employee compliance can be tracked and measured. They can also be used to train new employees and as a repository for employee experience and institutional knowledge.

Procedures detail the "how" and sometimes the "who" action to be taken in a

- Provide detailed instructions on the appropriate action.
- Can change frequently.
- Tell the "how" and/or "who."
- Address a particular process.
- Define the specific result to be achieved.

HOW TO CREATE AND MANAGE POLICIES AND PROCEDURES

This section provides guidance for organizations that do not have a formal process already in place. If your organization has a current process for creating and maintaining policies and procedures, compare your process with the best practices discussed in this section to ensure that they will be useful in an emergency situation. The guidance in this section for policy creation and maintenance also applies to creating procedures.

POLICY AUTHORITY AND RESPONSIBILITY

Ultimately the top operations executive—usually the chief operating officer (COO)—must be responsible for all policies governing the organization. This person should designate a policy manager or team to administer the creation and management of policies, which are reviewed and approved by the executive. The responsible executive's name should be on all approved policies to reinforce the importance of the policy.

If your organization does not currently have formal policies, the first policy should be to establish the importance of the policies, identify who has the authority to create them, and the consequences for not following them.

POLICY CREATION AND APPROVAL PROCESS

To enforce the importance of your policies you will need a formal process for creating and approving new policies. This process should document the creation, review, acceptance, and updating of a policy and give everyone affected by the policy a chance to participate in the process. You must involve those who are affected by the policy; not doing so will hinder acceptance and compliance.

Your official policy creation and approval process should cover the following steps:

- Explain how policy suggestions are made and by whom.
- Explain how policy suggestions are reviewed. If a suggestion is rejected, make sure the requester understands the reasons.
- The policy manager should assign a priority to the policy.
- The policy manager's team researches the requirements for the new policy and creates a draft policy.
- The draft policy is reviewed by management and the requester.
- After updating with feedback from management and the requester, the draft policy is sent to all interested stakeholders for review and comment.
- Comments are reviewed and incorporated in the policy, if appropriate.
- The new policy is sent to the responsible executive for review and signature.
- The new policy is posted and made available to the entire organization.

ORGANIZATION AND FORMAT

Policies must be organized in such a way that they can quickly be found when needed and for easy updating. An online document management system allows for ease of searching and maintenance, but be sure that you can access the policies in the event of a disaster. This can be accomplished by storing policies (or copies of them) in the cloud or by providing hardcopies for key team members to keep at home.

The layout of a policy should make the policy easy to read and to find information in the policy quickly. The policy team should develop standards for the formatting of policies and what information must be included. A policy will typically include descriptions of the following:

- The purpose of the policy
- The organizational scope of the policy
- What the policy covers and does not cover
- Background information on why the policy was needed
- The policy itself
- Any procedures that are defined to support the policy
- A history of revisions that have been made to the policy
- References to any supporting documents

Your policy team should determine which sections are required and which are optional. The purpose, scope, and policy details should be included in all policies.

IMPLEMENTING POLICIES

All managers are responsible for adherence to policies in their area of responsibility. This includes ensuring that new employees receive training on all policies that affect their role, and that existing employees review all policies at least annually for any changes that may have occurred in the previous year.

Managers must also work with their teams to identify issues or potential improvements to policies and report them to the policy manager.

Creating policies is time and resource intensive. You will only receive a return on this investment if the policies are known and followed. Employees will follow their manager's example; if managers refer to and follow your policies, then so will they.

POLICY MAINTENANCE

To be useful in an emergency, policies must be kept up to date. All policies should be reviewed at least annually, and more frequently for policies in areas that change rapidly. The review should follow the same process as the one used to create the policy. As technology and business changes, so must the policies governing them.

DETERMINING WHAT NEEDS A POLICY

There are many reasons to create a policy. Policies reinforce what's important to the organization and help employees understand the limits of their job without having to discover that for themselves. They also allow managers to focus on the exceptions that occur without having to micromanage employees.

The benefits of creating well-crafted policies include:

- Ensuring regulatory compliance
- Providing consistency in operations
- Preventing ambiguity about how to handle certain situations
- Promoting harmony in the workplace
- Managing risks
- Establishing a basis for continuous improvement
- Providing legal protection

Any area that is affected by any of these benefits is a good candidate for being addressed in a policy.

BUSINESS CONTINUITY PLANNING POLICY

The first policy that you will need is to establish the requirement for a business continuity plan (BCP). This policy mandates the creation of a BCP and what it should include. The following sections discuss what specifically should be included in your BCP policy. A sample BCP policy is shown in Figure 15-1.

BCP POLICY INTRODUCTION

Your BCP policy should start with background information justifying the existence of the policy and the importance of the policy to the organization. It should also state who has the authority to create the policy and may outline penalties for when the policy is not followed.

BCP POLICY SCOPE

The scope of the operations covered under the policy is stated here. It should make clear which parts of the organization are covered and which employees are affected, if appropriate. It might also specify areas of the organization that are not covered under the policy if applicable. In most cases, a BCP policy will cover all critical resources and processes.

BCP POLICY HISTORY

As is best practice with any documentation, a history of the policy is maintained in this section, including when the policy was first created and any nontrivial changes since. The policy history should show clearly how the policy has changed over the years and how "the way things are done around here" has changed over the life of the policy.

BCP POLICY

This is the meat of the policy, where the details of the policy are presented. Your BCP policy should be structured according to the following outline, with the exact language tailored to your particular organization's needs.

IDENTIFY CRITICAL RESOURCES AND PROCESSES

A Business Impact Analysis (BIA) and a risk assessment must be performed for each key process and system used in their area of responsibility. Each critical system and source of data for these systems must be identified and the importance to the organization documented. The BIA and risk assessment must identify:

- Processes necessary for the organization to function
- Financial impact for the loss of a system or process
- Regulatory or legal requirements impacted by the loss of a system or process
- All natural and man-made risks to critical systems and processes
- The recovery time objective (RTO) for each system or process
- The recovery point objectives (RPO) for data and other applicable resources

CREATE A BUSINESS CONTINUITY PLAN

A BCP must be created for every critical business function that is identified in the BIA. The BCP must include the following:

- Information on steps required to restore systems and processes identified in the BIA
- Prioritization of business function recovery after a disaster

- Steps necessary to restore access after a disaster at a recovery site
- An emergency notification plan for executive management and department heads
- Documentation on how the plan will met the RTO and RPO for each system or process

MAINTAIN AND TEST THE PLAN

The director of each department is responsible for ensuring that the BCP is kept up to date and tested on a regular basis. What follows are the minimum requirements:

- The BCP must be reviewed annually for new or changed natural, man-made, or technical risks.
- Mitigation plans must be reviewed annually.
- The BCP must be updated within 90 days of the go-live date for any new system or process.
- The BCP must be test every six months and evaluated for compliance with recovery time and recovery point objectives.
- Test results must be delivered to the COO within 90 days of completion.

TRAINING

All of our planning will be for naught if employees are not clear on their roles and responsibilities when a disaster occurs. All new employees must complete disaster recovery training within 60 days of joining the organization or a new department.

BCP POLICY AUTHORITY

This section is used to document who has the authority to approve changes to the policy. It may be the same person who originally authorized the policy, or this authority can be delegated to someone whose role is to coordinate policy changes. Include their name, title, and several ways in which they can be contacted.

The higher up the policy authority person is on the org chart, the more likely the policies will be followed.

POLICIES THAT MAY AFFECT DISASTER RECOVERY

Your organization may have a robust collection of policies and procedures that thoroughly cover your operations, but they may not address issues that arise during disaster recovery efforts. Policies and procedures that work well during normal operations may, if followed, hinder your ability to quickly and efficiently recover from a disaster. Extraordinary times call for extraordinary measures, and your various policies should be ready to deal with a disaster when one strikes.

ATTENDANCE POLICY

Your current attendance policy likely stipulates when employees should be in the office, specifying work hours, penalties for being late or absent, and how your supervisor must be notified. Attendance policies are designed to encourage employees to come to work. But blocked or icy roads, downed power lines, or other issues may make it too dangerous for employees to come into the office. During a disaster recovery effort, the office might not be safe or accessible and normal channels of communication may not be available.

Your attendance policy should address how employees will know to come to the office or stay home when a disaster has occurred, and give them guidance for making the decision themselves if needed. The policy should assure employees that the company has their safety in mind and will not penalize them if a disaster makes it dangerous for them to come to work.

FIGURE 15-1. BUSINESS CONTINUITY AND DISASTER RECOVERY POLICY

Effective Date: July 2014
Last Revised: March 2016

1. INTRODUCTION

"Company" requires that plans be created to ensure that operations can continue or quickly recover following the loss of service or resources due to a major interruption. Our customers, vendors, employees and other stakeholders depend on us to provide our goods and services as promised. This Policy defines who is responsible for protecting the organization's assets by planning for a disaster and what needs to be done to ensure that Company can continue operations after a major disaster.

This policy was created by authority of the Chief Operating Officer (COO), who is responsible for operations of the organization.

2. SCOPE

The policy encompasses all IT and business processes used in the day-to-day operation of the organization. Every employee in the organization is responsible for understanding their role in following this policy.

3. POLICY HISTORY

Date	Description of Revision
July 1, 2013	Initial creation.

2016	BIA.

4. POLICY

The Director of each department within the organization is required to create, maintain and test a Business Continuity Plan for their area. The following activities must be performed:

A. Identify Critical Resources and Processes

A Business Impact Analysis (BIA) and a risk assessment must be performed for each key process and system used in their area of responsibility. Each critical system and source of data for these systems must be identified and the importance to the organization documented. The BIA and risk assessment must include:

a. Identify processes necessary for the organization to function

b. Financial impact for the loss of a system or process

c. Regulatory or legal requirements impacted by the loss of a system or process

d. Identify all natural and man-made risks to critical systems and processes

e. The Recovery Time Objective (RTO) for each system or process

f. The Recovery Point Objectives (RPO) for data and other applicable resources

B. Create a Business Continuity Plan

A Business Continuity Plan (BCP) must be created for every critical business function that is identified in the BIA. The BCP must include the following:

a. Information on steps required to restore systems and processes identified in the BIA

b. Prioritization of business function recovery after a disaster

c. Prioritization of all critical technologies

d. Steps necessary to restore access after a disaster at a recovery site

e. Create an emergency notification plan for executive management and department heads

f. Document how the plan will meet the RTO and RPO for each system or process. The BCP must be reviewed annually for new or changed natural, man-made or technical risks

C. Maintain and Test the Plan

The director of each department is responsible for ensuring that the BCP be kept up to date and is tested on a regular basis. What follows are the minimum requirements:

a. The BCP must be reviewed annually for new or changed natural, man-made or technical risks

b. Mitigation plans must be reviewed annually

c. The BCP must be updated within 90 days of the go live for any new system or process

d. The BCP must be test every six months and evaluated for compliance with recovery time and recovery point objectives

e. Test results must be delivered to the COO within 90 days of completion

D. Training

All of our planning will be for naught if employees are not clear on their roles and responsibilities when a disaster occurs. All new employees must complete disaster recovery training within 60 days of joining the organization or a new department.

POLICY AUTHORITY

Questions or comments about this policy should be directed to:

George Jenkins, COO

Our Company, Inc.

6600 Company Drive

Columbus, OH 43215

Voice: 614-555-1234

Fax: 614-555-1235

gjenkins@company.com

In the aftermath of a natural disaster such as a tornado or hurricane, employees may be doing a lot of cleanup and repairs at their homes. If they are able to come to the office, consider being flexible with your dress code and working hours. Giving employees some flexibility to take care of things at home can help reduce their stress while at the office, making them more productive. Your attendance policy should address issues such as:

- What happens if an employee is asked to come to the office to assist with the recovery effort but refuses?
- Does the attendance policy take into consideration the employee's situation at home, such as damage to their house or injuries to their family?

SICK LEAVE POLICY

Sick leave policies typically cover what sick leave can be used for, how it is accrued, and how to use it. Usually a medical excuse is required if sick leave is used for a certain number of consecutive days. Employees are in many cases encouraged to get back to work as soon as possible.

After a natural disaster, many of your employees may be called on to provide specific kinds of emergency services at the local, state, or national level. Employees with medical, nursing, paramedic, firefighting, law enforcement, military, or other skills may volunteer or be called on to assist authorities in the case of a wide-area disaster. They may also be victims of the disaster and not be able to return to work immediately.

Consider how your organization would like to handle these situations and make sure that they are documented in your sick leave policy. Determine ahead of time what situations will be covered and how much additional sick leave the organization is willing to provide employees in these situations. Situations to consider include:

- How the sick leave policy will apply during a pandemic
- Whether an employee should stay home if a family member is affected by a pandemic
- Whether available sick leave or vacation time can be used if a pandemic is declared or if an illness such as the flu is common in the area

AFTER-HOURS ENTRY POLICY

Your after-hours entry policy likely is very restrictive when it comes to access outside of normal working hours. During recovery efforts after a disaster, employees may be working around the clock to recover and to catch up on work missed due to the disaster. Security may also need to be increased as damage to your buildings may have created additional ways that the buildings can be entered. Various doors and gates that are normally closed may have been forced open by emergency responders and the security mechanisms damaged. If new security personnel are required, they will need to be trained, and it will take some time before they easily recognize employees.

Make sure your after-hours entry policy covers how entry will be controlled when recovering from a disaster. If you have outsourced physical security to an outside vendor, review the disaster recovery section of your after-hours entry policy with them to ensure they understand your requirements of them in the aftermath of a disaster. Make sure that they understand your policies covering:

- How an emergency is declared
- Who has authority to grant emergency access
- How the emergency access list is managed and accessed
- Types of acceptable identification during recovery
- Special tracking of people during recovery
- Access to locked rooms

PAYROLL POLICY

Employees will be under enormous stress after a natural disaster, and the last thing they should have to worry about is getting paid. Exempt employees must be paid their normal wage, whether or not your organization is open after a disaster. If the workplace is open but exempt employees are not able to get to the office, the employer can choose whether or not to pay them or force them to use vacation or other paid time off.

Nonexempt employees are only required to be paid for the actual hours that they work. The Fair Labor Standards Act (FLSA) requires that nonexempt employees must be paid at least the federal minimum wage for each hour that they work and paid overtime for every hour after 40 hours during the workweek. So, if the workplace is closed after a disaster, there is no requirement to pay nonexempt employees.

Your payroll policy should include how the organization will handle the paying of employees after a disaster. Consider the impact on the morale of employees if their income is impacted due to no fault of their own. Many employees will be living from check to check, and a disruption in their income may be very stressful. This is particularly an issue if your organization is the only one affected (such a damage from a fire); employees whose income is interrupted may be quick to look for employment elsewhere, taking with them valuable skills and knowledge. The cost of continuing to pay employees whether or not they can come to work may be less than the cost of hiring and training their replacements.

Another potential issue to consider is what to do if your payroll and/or timekeeping systems are offline after a disaster. Plan ahead for not having access to these systems and determine how employees can still receive an income. The easiest solution may be to simply write payroll checks by hand (or pay in cash), with the amount based on the employee's net pay in previous periods. This can be tracked by hand and then reconciled with the actuals calculated by the payroll system once it becomes available.

You should not wait to address these issues until a disaster strikes. Plan in advance how you would like to handle these issues and make sure your payroll policy clearly reflects the decision. Consider including in your payroll policy:

- How payroll will be processed if the payroll system is unavailable
- Whether nonexempt employees are paid if they are unable to work during

Whether nonexempt employees will be asked to assist with recovery as a condition of being paid

WORK-FROM-HOME POLICY

No matter what your normal work-from-home policy states, during a disaster it may be advantageous for employees with access to the Internet to work from home. Traditional work-from-home or telecommuting policies place limits on who can work from home and under what circumstances. You might also have procedures that require employees to notify their supervisor and have the request approved in advance. There may also be limits on the number of consecutive days that an employee can work from home.

In the aftermath of a disaster the regular workspace may not be available or have limited access. Your work-from-home policy should address who might be required to work from home and also when employees who are stuck at home should not work if the bandwidth of your Virtual Private Network (VPN) is limited. Your policy should document which areas for the organization have priority in using the VPN after a disaster. The following is a typical hierarchy:

- Executive management, legal team, corporate communications, and the core Human Resources team—typically recovered near the Command Center and the disaster site
- The remainder of the Human Resources function, at the office recovery site
- Customer contact team (Sales)
- Accounting (important for maintaining cash flow)
- Company operations

Requiring approval in advance might also be waived during disaster recovery. Also, be sure to have a plan to check in periodically with employees working from home to keep current on their situation and to help get them back in the office as quickly as possible.

You should also consider how employees might be able to help in the recovery effort and what the organization should expect from them. Your work-from-home policy should clearly document these expectations so that there is no confusion after a disaster. Consider including in your work-from-home policy:

- How the decision to work from home is made
- Special considerations for using confidential information at home
- How attendance is tracked for employees working from home
- Any special considerations for employees that are single parents
- Flexibility in when hours are worked, to allow for dealing with issues at home

VACATION POLICY

There are several issues to consider when reviewing how your vacation policy can impact your disaster recovery efforts. For example:

- Anyone returning from vacationing in an area with known health risks should work from home for a few days before coming back to the office.
- Can planned vacations be interrupted if an employee with special skills is needed to assist with the recovery effort?
- Should you restrict where key employees can go while on vacation and discourage travel to areas with potentially serious health risks (e.g., Ebola and the Zika virus) or areas with serious civil strife?
- Backup plans should be implemented when key recovery personnel are on vacation and a disaster occurs.

EMPLOYEE ASSISTANCE PROGRAM (EAP) POLICY

Review your Employee Assistance Program (EAP) policy to ensure that it spells out what assistance is available to employees after a disaster. Employees who would normally have never used this program may find themselves in need of counseling or other services to help them recover in their personal lives. A wide-area disaster will have likely impacted your employees, their homes, and their families. Make sure your program includes assistance with issues beyond the immediate workplace so that they can get back to normal and become productive as soon as possible.

Participation in the EAP usually does not jeopardize job security or promotional opportunities, but it can affect an employee's availability during the recovery effort. Plan ahead for how you want to handle EAP participation during your recovery. Things to consider include:

- How to handle confidentiality issues when an employee is critically needed for the recovery effort but is seeing an EAP counselor during the hours needed
- Referring employees whose mental state has been affected by the disaster
- Impact on the employee's status if they refuse to participate in the EAP if referred by their supervisor

RECORDS DESTRUCTION AND DATA RETENTION POLICY

A records destruction and data retention policy (see Figure 15-2 for an example) can make your recovery planning a bit easier. A well-written policy will clearly document what types of records you expect to keep and where the records are stored. If these policies are being followed, you should have fewer issues around what to try to save and what can be safely disposed of during the recovery. Be sure that your emergency procedure for reporting accidentally destroyed records agrees with your overall records destruction documentation policy.

FIGURE 15-2. RECORDS RETENTION AND DESTRUCTION POLICY

1. INTRODUCTION

"Company" requires that plans be created to ensure that documents, records and other data received and created by the company are managed and protected. Many types of records are subject to laws specifying how long they must be retained by the company. In addition, the company incurs significant costs in the storage and protection of these records, and therefore requires that these records be destroyed when no longer needed for internal use or for satisfying legal requirements. This policy was created by authority of the Chief Operating Officer (COO), who is responsible for operations of the organization.

2. SCOPE

The policy encompasses all documents, records and other data received and created by the company. This includes records in all forms and throughout their lifecycle. The types of records covered by this policy include but are not limited to:

A. Legal records

This includes all records concerning the legal operation of the business such as vendor and customer contracts, copyrights, trademark registrations, patents and other corporate records.

B. Personnel records

This includes employment and personnel records of all kinds, including resumes, performance evaluations, employment contracts, and termination records.

C. Tax records

This includes all returns and any documentation required to verify the information included in the tax returns.

D. Accounting records

This includes all documentation to support business transactions recorded in the accounting system. Includes but not limited to sales receipts, expense receipts, etc.

E. Business communications

This includes any communications that might be subject to discovery in legal proceedings. The majority of these communications are in the form of emails or instant messages.

3. POLICY HISTORY

Date	Description of Revision
March 12, 2015	Initial creation.
August 14, 2016	Clarified what is included in personnel records.

4. POLICY

The company requires that all business records be retained for some time as determined by the type of record, then destroyed when no longer needed. All records are required to be marked with their type and optionally with their retention period. The retention period for each type of record is listed below:

Record Type	Retention Period
Accounts Payable ledgers and schedules	4 years
Accounts Receivable ledgers and schedules	4 years
Personnel Records	6 years
Annual Audit Records, including work papers and other documents that relate to the audit	7 years after completion of audit
Bank Statements and Canceled Checks	7 years

Interim Financial Statements	7 years
Notes Receivable ledgers and schedules	7 years
Investment Records	7 years after sale of investment
Internal Audit work papers and findings	7 years after completion
Contracts	7 years after expiration
Legal Records	10 years after close of matter
General Correspondence – Non-routine	Same period as the document they pertain to or support
Annual Audit Reports and Financial Statements	Permanent
General Ledgers	Permanent
Corporate Records	Permanent
Tax Records	Permanent

All paper records must be destroyed by a licensed service provider that can destroy the records onsite. The destruction of the paper records must be monitored by company personnel.

Disaster Recovery Considerations

During disaster recovery efforts all documents that are not marked will be destroyed. Damaged records that are marked will be sent to the document restoration vendor designated in the business continuity plan as quickly as possible. If possible, a record of all documents that are too damaged to be restored should be created and sent to the corporate records manager.

5. POLICY AUTHORITY

Questions or comments about this policy should be directed to:

George Jenkins, COO

Our Company, Inc.

6600 Company Drive

Columbus, OH 43215

Voice: 614-555-1234

Fax: 614-555-1235

gjenkins@company.com

During a disaster recovery effort your resources for restoring data may be limited. Your data retention policy should address the relative importance of data and what must be restored and what can wait, or what can never be restored. Some items you may want to include in your policy:

- How to handle out-of-date or unmarked documents
- Methods for documenting records too damaged to restore

SOCIAL MEDIA POLICY

During normal times it makes good business sense to have a social media policy to protect your organization's reputation and brand image. Most if not all of your employees are using social media in their personal lives, and they require guidance on what is and what is not appropriate to share on social media about their jobs. During normal times you may be encouraging them to share their positive thoughts about your organization to help raise awareness of your brand.

During an emergency and recovery effort, however, you will want to be more careful about what is being shared with the outside world. News media personnel your customers. Suppliers may be confused about whether they should continue making deliveries and may have concerns about getting paid. In a just-in-time world, your customers may question whether you can deliver the product they need when they need it.

To avoid confusion and misinformation, include in your social media policy that no information about the disaster or recovery should be made by unauthorized personnel, including but not limited to:

- The damage done by the disaster
- Status of the recovery effort
- Working conditions or hours
- Contractors assisting with the recovery

PURCHASING POLICY

Your purchasing policy likely spells out controls to carefully manage how the organization's money is spent. This may work fine during normal times, but during a disaster items may need to be purchased quickly to control the damage and to restore operations as fast as possible. Make sure your purchasing policy allows for certain products and services to be purchased without going through the normal approval process, both immediately before as well as after a disaster. Things to consider include:

- Defining when emergency purchases can be made
- Allowing department heads greater authority to make purchasing decisions when an emergency is declared
- Defining under what circumstances to delegate emergency purchasing authority
- Providing a list of approved emergency/disaster vendors for guidance in purchasing emergency/recovery items
- Directions on how to document emergency purchases
- Dollar limits on emergency purchases
- How emergency purchases are reconciled once the Purchasing department is back in operation
- Guidance on when equipment for emergency use should be leased or rented rather than purchased

CONCLUSION

Policies and procedures are a critical component of the recovery effort. They provide important guidance for activities not specifically covered in the business continuity or disaster recovery plans. All company policies and procedures should be reviewed to ensure that considerations are made for disaster situations.

Policies and procedures must be reviewed regularly. Processes change over time, and a regular review will catch updates that have not made it into the policies and procedures.