Version 1.0

Date: 10/5/2019

Data Backup Policy Template

1. 0 Purpose

To provide our members a template that can be modified for your company's use in developing a Data Backup Policy. This backup policy template compliments the NCSS's guide titled "How to Create a Backup Plan" found on our website under How-To-Guides. This policy template focuses on codifying your backup strategy.

2.0 Backup Strategy

Define your backup strategy in the policy. Explain how employees are to use the following storage locations and what should be stored at each location.

A. Local Copy. In this section provide guidance on what employees can and cannot store on their workstations, laptops and personal devices. **NEVER ALLOW** employees to store business data on their personal device.

B. Local Backup. In this section of the policy document, establish the methodology and location of where employees should store business data locally such as a server. Define the structure of the file - often businesses use record management procedures to name the files. ISO 15489-1:2016, is the international standard for record management and defines the principles and approaches to create, capture and manage records. See the attached link for more information:

https://webstore.ansi.org/Standards/ISO/ISO154892016?gclid=EAIaIQobChMIyqL2_d285AIVCRgMCh1gTwqTEAAYAiAAEgLn1PD_BwE

C. Offsite Backup. In this section, define what should be stored offsite, how often it is backed up, where the storage location is and the provider of the service. An offsite location is helpful in the event the business location is compromised by fire, vandalism or theft. A remote site could be in another state or county. These backup services typically copy all data after the end of the business day. A service provider may use tapes or other means to store the data. Often businesses who are prone to weather outages from hurricanes, floods or other natural disasters, back up their data outside the threat prone area.

3.0 Data Backup Procedures

In this section, define the means by which your workforce backs up your business data. It is a good time to brush off your data inventory audit - which should list all the data your store, the sensitivity and controls to protect it.

Data Backup Policy Template

Any data that's critical to keeping your business running should be backed up. Financial records, customer records, tax forms, sales records, websites files, software, and project plans are all examples of critical data to back up. During the data audit, your team should identity all sensitive data that needs to be maintained and backed up. This data will need to be encrypted whether it is stored locally or offsite. Access to these files should also be controlled through access control procedures – like identity authentication and verification (login in name, password, as well as two factor authentication).

Define the procedures your employees must use to back up data. For example, if your accountant submits financial records for monthly or yearly closeout, define how your staff would store it and where - there might be a local file copy and a backup copy at an offsite location.

Remember that having your business data only in the cloud is a single point of failure. Plan to have your data stored locally and an offsite location. Some small businesses routinely store a copy on removable hard drives. Ensure these storage devices are locked up.

Five years is usually the maximum time required to keep data. The "Data Protection Act" requires personal data processed for any purpose "shall not be kept for longer than necessary for the purpose." This act states the maximum period of retention is regarded as 5 years. For this reason, it is critical to capture the date of origin of the data (like in the file name), such as *BalanceSheetNCSS0123118.*

4.0 Backup Schedule

In this section of the document define the periodicity of backups. This section would cover backups at a remote location by a service provider. One item to note - criminals who infect your systems with ransomware are now turning to deleting backups. So it's important to talk to your service provider to ensure that your company is protected from a criminal accessing their site to destroy your data.

The best time to backup is whenever data changes, so a continuous backup system is the best. Most backup systems work by backing up all of your data once, and then incrementally updating only what's changed or new. Also think about whether you need a backup of your backup. Some businesses make a point to rotate their backups periodically to make sure that even if one backup fails, another can take its place. How much redundancy you want or need is dictated by how much time, money, and equipment you're willing to invest. Your backup service provider can assist in determining your best strategy. So it's best to use this section in the policy document to define the services the backup service provider delivers to your business and points of contact, phone numbers, and emergency contact phone numbers.

Data Backup Policy Template

5.0 Data Recovery

In this section define how the data would be recovered from the backup. The document should be a step-by-step outline of:

1) what systems to bring on line first;
2) what data files need to be restored and in what order: and
3) testing of the system and data files through each phase.

Define who will lead the data recovery process, who will verify the systems are functioning as required and who will verify the data files are current and accurate as of the last backup.

6.0 Data Retention

Lastly, the document should include a section on data retention policies for the company. You may want to consider having a separate data retention policy for your business, and if you do, reference it here. The retention schedule lists the type of data, the record name, how long the record will be maintained and when and how it will be destroyed.

7.0 Applicability

A. This policy is applicable to all company employees and all official corporate records.