Toolkit Template
Employee Training for Processes and Security

Objective: This template has been developed to document critical activities and information related to your business in the event of the incapacitation of your executive leader or owner. This Toolkit Template provides a guide for properly training employees for company processes and security protocols.

Introduction

Business Operating Expense (BOE) policies are designed to help a business survive the incapacitation of a principal member of the business by reimbursing some fixed expenses. However, the policy alone will not ensure survival of a business; organization and preparation are essential, requiring proper processes and security be in place and appropriately documented.

Processes and cyber protections, while seemingly disparate, are closely allied. Cyber protection requires vigilance, consistency and predictability--the role of processes. And, processes that do not incorporate good cyber protections fail the company by not protecting critical assets.

Processes

Well-designed and documented processes serve the business by providing a consistent, repeatable, predictable, and transferable method of performing business functions. "Consistent, repeatable, and predictable" mean that a process begins with the same inputs, employs the same steps, and ends with the same outputs regardless of who performs the process. "Transferrable" means that anyone properly trained will be able to complete the process successfully.

Creating—actually documenting—your processes comes first. Please see the Toolkit document Business Processes and Documentation for more information.

In essence, processes should be defined for all business tasks. Many businesses, especially small businesses, feel people know what to do and new employees will be shown by existing, experienced employees. Without defined processes, each employee can do things their own way. This makes it more difficult to create uniform and consistent outputs, or recreate an error situation to correct it. And note—with each person performing a task his or her own way it is difficult to maintain effective cyber security protections.

In addition to creating consistency in the performance and output of business functions, processes help protect the company's information, including that of clients, customers and patients. Not only does this make sense, it is legally required in healthcare, financial services, and some other industries.

By defining processes that incorporate cyber security best practices, the outcomes are predictable and compliant with legal regulations.

Once the processes have been developed and checked for completeness and legal compliance, ensure employees performing the process and their backups are trained on how to perform the process. The business owner and/or operations manager needs to be familiar with, and trained in, all the processes.

These steps may be considered basic or inherently understood, but in the event of activating the Business Operating Expense policy they are essential since people may be called upon to perform roles usually covered by someone else.

Cyber and Regulatory Compliance

With the growing cyber threat, it is critical to make certain that proper security measures are being taken to protect business-critical and legally-protected information acquired, stored or accessed by computer.

Cybersecurity regulations are expanding to include more information and to intensify the responsibility of companies gathering this information. Personally Identifiable Information, PII, and Protected Health Information, PHI, are legally regulated and must be protected at all times. PII includes any information which can be used to identify a specific person. PHI includes personal information about a person's health. The healthcare and financial services industries are bound by strict regulations, but protection of information is essential regardless of industry. It is not only a requirement; it is just good business! Trust is an important aspect of business continuity. Companies not exercising sound judgement in protecting client information will lose clients' trust. Additionally, regardless of legal requirements, cyber insurance firms may look at how you protect customer information before determining if a claim will be paid.

Information Technology gets the most press and attention for cyber risk. However, research from Verizon's 2018 Data Breach Investigations Report shows over 50% of breaches and incidents have human causes. Human error covers a wide range of activities, from clicking on bad links to failing to patch computer software, to falling for phishing schemes, failing to follow approved procedures, and many other reasons. But the results are the same--compromise of security and loss of information. Well-designed processes and training are strong and effective ways to combat this.

Creation of processes should be overseen by two constituencies: the business to ensure it is complete and accomplishes the business need; cyber security professionals to ensure it meets best practices and legal requirements for protecting information.

The next step is to be able to prove compliance to regulators and cyber insurers. In order to do this, the training process must be documented showing:

- The title of the process(es) covered
- The training material(s) presented
- The employees attending the training
- The subject matter covered
- The dates of the training
- If each employee was tested on the covered material and a copy of the test
- The score achieved by the employee
- Sign off by each employee and the instructor

Processes and training are important but effective means of enforcing the processes is critical. This means oversight in how employees perform the tasks; do they follow the approved processes or not. And if not, strong measures must be in place as an incentive. If the enforcement measures are not created and themselves enforced, there is no point in creating the procedures or the training. People will just revert to doing it the way they want.

Closing

Periods of crisis and stress are not the times to begin defining processes or training employees. Remember, the company issuing the BOE policy wants to know that the business will remain viable in the event of policy activation and may want to see the same proof as regulators. Even if the policy issuer does not review this, you as the company owner or principal want to do all you can to ensure the continued functioning of your company.

Begin this work as soon as possible as no one can predict the future.