Information security policy essay sample

Law, Security

Sunica Music and Movies will be implementing a full security plan to ensure proper handling and access of data in our new system. Vulnerable customer information being properly protected is a top priority for us. An added benefit will be the security and accuracy afforded to employees through this protection.

Customers trust this organization with highly private personal and financial information. That makes it our responsibly to handle that information with the utmost respect and care. Through the controls and procedures outlined in this policy we can achieve those goals.

Employees have the right while being given access to this type of information to also be fully protected. The controls and procedures designated here will also facilitate that. For example leveled access removes temptation to lower level employees and protects them from being accused of infractions not ever in their control.

Here at Sunica we are ready to keep up with technology and build a better business model through that practice. However without a complete security outline and the enforcement of it we will not achieve this goal. It is highly recommended that this policy be carefully read and followed by all parties involved in this company. A signed copy will be required to be kept on file for all employees and customers will be made fully aware that their security is our top priority.

Introduction

1 Company overview

Sunica Music and Movies is a small business that is making a move to keep up with technology. The goals of this company are to synchronize the many locations to work together as one and develop a web presence. To accomplish these goals they are going to link the stores with private business data on one side and a user interface for the public on the other. Inventory and accounting will be a large factor in their success but security will be a very important aspect as well. Since transactions are conducted online they will require security from the inside and outside of the system.

2 Security policy overview

As a small company a System-Specific policy will be appropriate. By clearly outlining data handling procedures for the system key factors like protection, detection and response can be maximized and provide an overall better level of security.

3 Security policy goals

1 Confidentiality

This company handles private and financial data so prohibiting misuse of this information is vital. There will be layers of access consisting of manager, asst. manager and cashier level employees.

2 Integrity

Credentials for each employee will be provided by management. Customers will create personal credentials to conduct transactions. Firewalls will keep things contained and immediate encryption will apply to personal financial information.

3 Availability

Back-ups will be required daily and equipment protected to the extent of our ability against disasters natural or otherwise. Equipment will be cleaned, maintained, and up-graded at appropriate intervals to help avoid failure.

Disaster Recovery Plan

1 Risk Assessment

1 Critical business processes

The mission critical business systems for Sunica Music and Movies include the web, accounting and transaction servers in the data center and the in-store devices that connect to them. Employees and customers rely on these systems to operate properly.

2 Internal, external, and environmental risks

Possible threats at Sunica are fire, earthquakes and human related. Fires happen for countless reasons and if either the store locations or the data center were to have one the damage could range from monetary (small and large) to loss of the life of a customer or employee. Earthquakes are also unpredictable and have the same range as fires for damage. Human related problems could come from employees or hackers but will mostly be theft related.

2 Disaster Recovery Strategy

The type of alternate site recommended for Sunica is the warm site. A warm site will cost less than a hot site and will allow systems to be restored in a more timely fashion than a cold one. As a medium sized company with limited resources Sunica could quickly set-up a back-up system utilize the location and links provided by a warm site with minimal effort to resume business.

3 Disaster Recovery Test Plan

1 Walk-throughs

Managers will highlight key areas that can be affected by each scenario and notate any specific problems found. The IT employees will be given a walkthrough of the warm site and briefed on specifics needed to launch it quickly and efficiently.

2 Simulations

Managers will learn to contact and work with IT staff through a periodic simulation of a given disaster so that they are familiar with each other prior to a problem. IT staff will run these different scenarios so that they are prepared to assist management with crisis situations.

3 Checklists

Checklists will be built during simulations and agreed upon with co-operation between IT and management. Each scenario will have specific response procedures through this exercise and changes will evolve with operational procedures.

4 Parallel testing

This type of testing will re-enforce what is learned during simulations with an actual test of the system while remaining online. The warm site will be setup by IT staff and switched to by management so that procedures are physically rehearsed.

5 Full interruption

A full interruption will not be necessary for this plan as the other types of testing should suffice to train staff to work together by knowing their roles and relying on each other to respond accordingly to any given situation.

Physical Security Policy

1 Security of the building facilities

1 Physical entry controls

As Sunica Music and movies is primarily retail locations all doors will use a dead bolt type lock. Only the manager and assistant manager will have keys. Upon entry and exit alarm code must be entered into the emergency control keypad or the police will be called. They will have different codes so that entry/exit is logged. Glass and doors can be set with breach detection sensors that will also trigger an alarm. Offsite data center will be secured in this same fashion but access will be for IT staff only.

2 Security offices, rooms and facilities

Cameras and motion detectors can be strategically placed inside each location. Camera footage will be recorded by a third party at an offsite facility. Motion detectors will trigger a call to the police. The manager's office will have a combination type door handle. A backup generator will ensure lighting, computer and alarm systems are secure. Fire detection will include heat and smoke detectors that alert the fire department. Sprinklers and power supply cutoff will also be triggered. Proper maintenance and a pre-determined emergency contact for HVAC systems will ensure computers are protected. Offsite data center will also be equipped with these measures and IT staff will be notified of incidents.

3 Isolated delivery and loading areas

These areas will also have cameras and motions sensors. Cameras will record all the time and it will be posted. Motion sensors will activate at night and trigger bright lighting so that cameras remain effective.

2 Security of the information systems

1 Workplace protection

Computers/registers will be linked and individual credentials will be used to access them, management and IT staff will write credentials; employee logins/logouts will also be recorded. IT staff will adhere to these policies at the data center as well as on-site with their own credentials.

2 Unused ports and cabling

Any ports or cables that are not being used will be reported to IT staff who will then terminate, block or monitor them by which action is appropriate.

3 Network/server equipment

In-store routing and associated network devices will be accessed by credentials and each position will have leveled access. Firewalls will protect against network intrusion. Servers will also have leveled access for IT staff. A RAID system will be put in place for data recovery. Adequate cooling systems are to be used on servers at all times.

4 Equipment maintenance

Specific manufacturer recommendations will be strictly followed for all computer and supporting equipment maintenance. Scheduled cleaning will also be strictly followed. Forms will be at each location for employees to communicate problems/repairs needed.

5 Security of laptops/roaming equipment

The only laptops used will be diagnostic/service laptops to provide IT staff increased mobility. These laptops will adhere to all other credential and firewall requirements noted. A sign in/out policy will record employee use. They will have remote access to servers but will store only necessary data, all other data will be transferred directly to servers. GPS tracking will be put in place to react to any thefts.

Access Control Policy

1 Authentication

Sunica Music and Movies will implement many authentication levels for employees and customers throughout our systems. Customers will access accounts via encrypted user names and passwords of their choosing when initial account setup takes place in order to maintain their privacy and secure their transactions. Store employees at designated levels will use multifactor authentication that at high levels will include biometrics to access systems. Customer service personnel will have cards that have to be swiped and PIN numbers to use to not only clock themselves in/out for their shifts but also to access registers/customer accounts. Only management will have passwords that allow changes to be made and IT staff will be required to submit fingerprints in order to access buildings servers are housed in. All of these logins will be recorded for a designated period of time. Single sign-on will keep things simple for customers and employees that utilize different systems periodically will also use it to improve efficiency.

2 Access control strategy

1 Discretionary access control

Once a customer sets up an account any information provided by them is owned by Sunica and therefore must be protected. Customer service personnel will only have access to information needed to facilitate transactions, management will access to all customer information and IT staff will not be permitted to view any specific customer information unless accompanied by management as it is not required for them to keep systems running.

2 Mandatory access control

This type of control will not be used at Sunica as it is most appropriate for government/military operations.

3 Role-based access control

This type of control will not be used because even though it maximizes time in an organization with high turnover at times, the security of our customer’s information is one of our top priorities and many financial numbers are saved in our systems.

3 Remote access

The only remote access this company deals with are diagnostic laptops that will require IT staff to sign in/out of the database facility and use their single sign-on credentials to operate so that use is logged directly to the user.

Network Security Policy

1 Data network overview

Sunica Music and Movies will utilize WAN technology to link all locations to a centralized database and therefore begin working in unison. The stores will no longer operate independently of each other in chaos. An Intranet will be used for private business operations to achieve this goal. The public Internet will be tied to this Intranet in order to provide better and more convenient service to our customers.

2 Network security services

1 Authentication

The process of authentication will ensure that systems both for employees and customers will be accessed genuinely by the proper individuals.

2 Access control

Restrictions of access will further ensure that company procedures are followed and customers are better served. These controls will also protect customer privacy and system integrity.

3 Data confidentiality

Only data necessary for specific employee levels will be available for business purposes and customer information will be separated for this purpose as well.

4 Data integrity

In order to maintain the integrity of data that is collected and/or stored all aspects of this policy will be strictly enforced.

5 Nonrepudiation

This is achieved by access controls and valid signature agreement of customers and employees to uphold this policy from the beginning of the mentioned relationships to Sunica.

6 Logging and monitoring

All access will be monitored and logged for the set amount of time appropriate to its nature. Also frequent or excessive use of a given system will be flagged and checked into by corresponding staff.

3 Firewall system

1 Packet-filtering router firewall system

A packet filtering router will be used in correlation with firewalls to ensure authentication protocols are being followed so that only registered users are accessing systems.

2 Screened host firewall system

Firewalls will protect the system from the inside and out by being specifically designed to allow only relevant properly requested or non-critical information to pass through.

3 Screened-Subnet firewall system

This technology will not be used as Sunica is not a large enough company to benefit from it.

References

Cite all your references by adding the pertinent information to this section by following this example.

American Psychological Association. (2001). Publication manual of the American Psychological Association (5th ed.). Washington, DC: Author.

None Applicable