**CS362 Homework #10**

Introduction Section

The purpose of this document is to protect the interests of ZedAuction and its business partners. ZedAuction is a respected Electronic commerce (Ecommerce) company, and as such, must be secure in order to do business with its customers. Policies introduced and enacted are for the best interests of the company, its employees, and its customers.

The Security Chair will oversee all security implementations, policies, and will be responsible for the effectiveness of those.

All employees, vendors, and contractors are expected to follow these policies and notify management if they find that a co-worker(s) is not. If any employee is found to be willfully circumventing guidelines, appropriate disciplinary action, up to and including termination, will be taken.

Policies Section

Purchasing policy – Everyone has budget they must follow

Equipment policy – Everyone must use the same and/or compatible equipment

Internet usage policy – Internet will be used for business functions. If something needs to be researched, full internet access can be requested. (e.g. Quota time)

Electronic Messaging policy – Electronic messages should only be used for business purposes. The company will monitor any communication with outside parties for virus detection.

Privacy policy – Employees can expect a certain level of privacy into what they do on company premises and with company property.

Backup policy – Work must be backed up. Since ZedAuction is all electronic forms, this is vital to recordkeeping.

Requisition policy – Employees will need to justify the need for any equipment ordered or services bought with company money

Purchasing Policy:

Each department of ZedAuction will have a budget that they need to follow as set by the financial department. Appropriate uses for the budget will be detailed below. Anything purchased will retain ownership to ZedAuction.

Internet Usage Policy:

Internet services are to be used for navigation around the company intranet. If access is needed to the internet proper, then a request may be made to a supervisor or the IT department to allow full access for research purposes (e.g. Quota Time). A virus check will conducted at maintenance on all machines that used Quota Time.

Asset Classification Section  
  
ZedAuction holds many assets to its name and must be able to determine exactly what those are. These include, but are not limited to: Hardware, software, personnel, sale information, customer goodwill, and finance information. A full list of assets can be found in the standards. All assets must be protected to ensure the survival and future growth of ZedAuction as a business. Protection of specific assets will be detailed in the standards.  
  
Risk Management Section  
  
ZedAuction will protect its assets to the best of its abilities. Audits will be done periodically to determine what assets will need as far as protection, preventative measures, and security protocols. These, after they are determined, will be defined in the standards. ZedAuction recognizes that no venture is 100% secure, but it does have the responsibility to get it as close to 100% as possible. Protection from data theft, personnel demoralization, hardware overtaxation, and company defamation are chief among ZedAuction’s concerns, but not it’s only ones. ZedAuction aims to be a secure bet for our potential business partners.

Security Awareness Training

Security is paramount to ZedAuction’s business. To maintain an appropriate level of security awareness with employees, all new hires will take a basic security training module to what is expected of the employees of ZedAuction. At regular intervals, employees will be re-trained in the module. If a new security standard is implemented, all employees will have mandatory training in the new standard.

Employees will also understand that there will be different clearance levels. A base employee will not have access to inner workings, such as granting internet privileges. A senior employee will have more access to projects and the inner workings, but not everything. Administrators will have access to everything for their department, but will not have access to other departments.

Security Model

The security model for ZedAuction is a layered security model. This means that certain applications will only have access or knowledge to certain areas of the business, as much as needed to perform their primary function. This is known as least privilege.

For the PayAll application, the only things it will need to know are how much money to send to each bank account routing number. No names need to be associated with account info, which if stolen, could lead to fraud. A senior member of the finance department will have access to modify, add, and remove accounts and modify pay grades. The Security Chair will have access as well, and a regular audit done by an outside auditor will be done so as to curtail any abuse of the system. Any glitches found will be high priority. Any substantiated abuse will result in termination.

Access Control

For ZedAuction, access control is important to only allow authorized personnel see and edit sensitive documents. Access will be done through role based methodology. Certain roles will have access to certain levels of documents. These permissions will help keep the systems ZedAuction secure and functioning for many years. The different roles will be listed in the standards.

Physical Access  
  
Access to the building is important since access to the building can mean access to the inner workings of ZedAuction and its assets. Building access shall be done via card reader. The cards read will be an individually issued ID badge. There will also be security guards near the front, watching for any suspicious persons or behaviors. The data center is to be protected via key code and security guard who will inspect your guest badge.

System Physical Security

The physical system shall be laid out as such: A workstation will be faced away from any windows so no peeking can be done. Workstations are to be kept neat; a messy station can get in the way and potentially be a fire hazard. All workstations are password protected, with passwords changed periodically.

System Network Security

The company will follow the OSI model for network security. This will provide an adequate level of security for the company.

Security Logs

Logs will be saved and archived. This is to help keep track of potential threats to the system.

Network Security Design

Servers will be kept in a secure portion of the facility, attached to UDP power sources in case of outages. There will be failsafe generators that kick on in case of outage to keep the servers running. Workstations are kept in a localized area, available to everyone who would have need of them. There would be a wireless audit done to determine how many routers are needed.

PayAll Remote Access

There will be no remote access for PayAll. It just leaves too much power out in the open to be abused

Secure Programming Environment

ZedAuction will make use of the spiral model of development. There would be tiers and roles for the development team. More important and critical stuff will be handled by fewer, more trustworthy members. Least privilege will be implemented.

Code Review

Code that is checked-in will be associated will a specific developer ID. This will narrow down, if not outright identify, where malicious code originated from.

BCP/DRP

There is need for backups and plans in case of emergency. Part of ZedAuction’s success lies in its continued operation, even if it’s experiencing technical issues. This is done by having a seamless transition to a backup hot site. This hot site will continue operations as normal while the main site is handling the problem. If this is not a feasibly cost effective solution, a mobile backup should be considered. In case those options are implemented and also go down, a mutual aid agreement should be set up with an outside company that continues our operations while we rectify the problem. Every hour that ZedAuction is down is $1,000,000 in lost revenue processes (figure is current as of writing). There should be backups, UDPs, generators, etc. as well to combat any power issues, corrupted drives, etc.

Forensics and Investigation

Crises are serious situations and should be handled accordingly. If they are not, ZedAuction and its customers could be at risk. Forensics relates to how to methodically work through legal problems. The biggest step is to document everything you find, so a timeline can be constructed from how events are recounted. Investigation relates to how to methodically find the problem that is plaguing the system. Data collection will be assisted by a contractor, but investigations will be kept in-house. The budget will be determined by the chief security officer and the chief financial officer. Security analysis facility will be kept separate from normal network operations so as to not corrupt the whole system. The thing everyone should know is that if a problem is suspected, notify the CIRT(Computer Incident Response Team). CIRT is trained bi-monthly for 40 hours per training period to accurately identify and resolve issues. They are like firefighters to a house that’s burning down. Notify them and do not get in their way.