Project#1: Employee Handbook (IT Security)

[Author’s name]

[Institute’s name]

Project #1: Employee Handbook (IT Security)

**Executive Summary**

Red Clay Renovations Company established its business position in providing suitable services for renovation and rehabilitation in the case of residential buildings and dwellings. The specific operational features of this company characterized as the “smart home” and “Internet of Things.” This organization is focused to utilize upgraded technological services to give the best architectural experience to potential customers. Data security management is one of the prominent departments of the organization that is closely connected with another operational unit (Simshaw, 2014). It is noteworthy to mention that there is the existence of specific security risks for the company when it comes to proper protection of the client’s information and addresses the threat of data breaching. The information technology management department must develop suitable IT policies to meet the standards of data protection.

**1st Policy: Acceptable Use Policy for Information Technology**

**Scope**

The implications of this specific policy consisted of all the authorized users who access information technology resources managed by the IT department of Red Clay Renovations Company. The overall IT system of the organization covers the comprehensive development of the company’s Information Technology Security program under the spectrum of ISO 27001/27002 requirements.

**Purpose**

The purpose of this policy approval draft is to explain employees’ obligations and responsibilities concerning the approach of information technology security in the organization.

**Policy Statement**

IT resources of the company play a critical role to broadcast important information about an organization’s operations to different departments. The primary goal is to deliver and expand the overall knowledge and information in the case of all the shareholders. The organization of Red Clay Renovation has a comprehensive IT security policy to successfully handle all IT related matters. The aim is to maintain an integrated IT system to effectively channelize all the organizational activities under the domain of proper practice.

           The broad approach of Red Clay Renovation Company’s IT system includes various physical domains such as electronic equipment, IT services, technologies, and the entire data used for information handling, accurate transfer, storage, display, and the overall IT communication platforms (Siau, Nah, & Teng, 2002). Computer-based instructional management systems, electronic devices, computer usage in the form of email, networks, telephone, voicemail, printing instruments, and electronic instructional materials characterized as the range of existing IT resource systems of the organization. Consideration of Owing Mills Facility functioning in the company also associated with the dissemination of information between different operating units.

**Acceptable and Unacceptable Uses of Information Technology Resources**

The employees need to have a proper understanding that what forms of information technology resources or permissible and what needs to be avoided. This form of understanding is vital to avoid any complication in the future and ensure the appropriate domain of IT resources handling. When it comes to the acceptable use of information technology resources of the company than all the employees of the company characterized as authorized users of the system. They can use information technology resources for managerial and business purposes considering the prospects of financial systems and the human resource department of the organization.

           Exploration of unacceptable use of information technology resources is also important to avoid any future discrepancies. It is forbidden for the employees to share or transfer business authentication information to external entities. Moreover, the use of credentials of others is also strictly prohibited under the legal policy of data protection of the company. Additionally, it is also important for the workers to follow different federal and state laws to avoid the risk of data breaching or improper use of the company’s information. The great range of unauthorized email messages is also not allowed to ensure proper protection of the internal data of the company.

**A Violations/Sanctions Section**

All the employees need to have a complete understanding that what can be the aftermath of failing the permissible use of information technology resources of the company. The failure to accomplish all the provisions of this policy may result in the immediate suspension of access to different IT resources of the company. Moreover, the legal spectrum developed in the organization has the authority to take strict disciplinary actions against the employee who falls in any form of data threat for the company. The facets of privacy and data protection laws are strictly applied to ensure the proper use of information technology data adhered to by the organization.

**2nd Policy: Bring Your Device Policy**

**Scope**

The policy regarding Bring Your Device (BYOD) is applicable for all company’s employees who intended to connect their information technological devices with the overall IT system of the organization.

**Purpose**

The core purpose of this policy statement is to explicitly define the company’s rules and regulations for all the employees concerning the approach of their smart technologies such as smartphones in the form of an organization’s network. It is the responsibility of the information technology management department to set instructions for the employees when it comes to using specific web browsers.

**Policy Statement**

Identification of suitable IT security instruments for the employees is a necessary paradigm to ensure the protection of internal data. This policy also intended to provide a proper plan of action to the employees when it comes to using their smart technologies within the vicinity of the company. The core aim of this perspective is to ensure the proper protection of the company’s data. The organization of Red Clay Renovation shows flexibility and allows employees to purchase and use different smart technologies at work for the sake of their comfort. The primary intent of this policy is to protect the information security of the organization under the domain of information technology infrastructure (Caldwell, Zeltmann, & Griffin, 2012). Specific terms and guidelines set for the employees under the spectrum of the BYOD program and any form of failure can cause strict action by the company.

**Acceptable Use**

* Acceptable business use of smart technologies and activities are clearly defined for all the stakeholders to ensure successful support to the company.
* When it comes to acceptable use of technologies that reasonable time is awarded for all the workers to meet their requirements of personal interaction and communication with others.
* Moreover, there are specific networking websites that are completed prohibited for the employees to use during work in the company.
* Personal technological devices can never be used to store the internal data of the company.
* Attaining or storing business information of any other organization is also not allowed under the risk of data theft or inappropriate business networking.
* Continuous engagement in activities other than business objectives is also under strict consideration.
* It is allowed for the workers to use smartphones but this approach should not affect the pace of work and all the tasks should be completed on time.
* All the connectivity problems need to be addressed by the IT department of the organization.
* When it comes to the use of devices than initially they must be approached to the information technology management system of the company. The objective of this consideration is to ensure the domains of job provisioning and configuration of different applications and security instruments.

**Security Dimensions**

     A detailed consideration of different security approaches under the practical scenario of the BYOD policy is also important to ensure data protection cases of both individual and organizational levels.

* Consideration of password to use devices is necessary to prohibit unauthorized access to information.
* All the devices need to be lock automatically with the approach of a password or PIN after some time.
* Rooted technological instruments need to be completely banned when it comes to accessing a specific network.
* All the smartphones used by employees for personal use should be connected to the company’s overall network.
* The operating information technology system of the company has the right to disconnect services whenever there is the detection of any form of risk.
* The workers must use all their devices ensuring the successful domain of ethical obligations and proper guidelines.

**3rd Policy: Digital Media Sanitization, Reuse, & Destruction Policy**

**Scope**

All workers of Red Clay Renovation Company have a critical responsibility to guarantees the confidentiality and protection of the company’s important information. This specific perspective is associated with the fair use of computer systems and different digital storage instruments as well as the consideration of non-reusable media. The broad perspective of digital storage devices comprised of elements of desktop workstation, laptop, server, smartphones, tablets, and the hard drives of all the computers. Consideration of external data storage instruments is also considered in the forms of disks, flash drives, CDs, etc.

**Purpose**

The main aim of this policy development is to direct all the employees concerning the main idea of licensed software programs and the protection of the data. It is essential for the employees to reliably erased the company’s data before it transferred to the outside areas.

**Policy Statement**

It is important to share proper and brief guidelines for all the employees working in different departments of the company. This central aim of this policy brief is to enhance the understanding level of employees considering the sensitivity of digital media sanitization.

* The stakeholders need to ensure that electronic storage media information needs to be sanitized once it is no longer in business use of the company.
* The priority areas of electronic storage media in the case of Red Clay Renovations Organization are mainly prioritized for the personal information of clients.
* A comprehensive application of shredding paper reports by the concerned department is necessary to meet the objective of sanitization in case of non-reusable electronic media before the domain of disposal (Golubic & Stancic, 2012).
* The heads of all the departments of the company are accountable to ensure the execution of proper sanitization in the case of all the workers.
* The involvement of the logistic services department is critical to meet the standards of disposal of computer media and other devices that are no longer in use of the company.
* Clearing data from various storage instruments is also essential to remove sensitive company information. These specific devices can be identified in the forms of thumb drives, hard drives, and CDs, etc.
* It is also essential for the concerned workers to ensure the removal of names, numbers, and addresses from phones, fax machines, and computer systems when it comes to sanitizing the devices.
* All the electronic information systems should not be released from the overall storage of the company once the process of sanitization can never be complete by following all the relevant rules and guidelines.

**Penalties in Case of Violations**

           It is also important for the decision-makers in the case of operations of these organizations to clearly defines the prospects of all the complications and penalties if the standards of sensitization and reuse of electronic devices are not met.

           The violation of this policy can cause the establishment of strict disciplinary action against the guilty individual. The severity of this perspective can be observed in the form of complete termination from the services in the organization of Red Clay Renovations.

**References**

Caldwell, C., Zeltmann, S., & Griffin, K. (2012). BYOD (bring your own device). *Competition Forum*, *10*, 117. American Society for Competitiveness.

Golubic, K., & Stancic, H. (2012). Clearing and Sanitization of Media Used for Digital Storage: Towards Recommendations for Secure Deleting of Digital Files. *Central European Conference on Information and Intelligent Systems*, 331. Faculty of Organization and Informatics Varazdin.

Siau, K., Nah, F. F.-H., & Teng, L. (2002). Acceptable internet use policy. *Communications of the ACM*, *45*(1), 75–79.

Simshaw, D. T. (2014). Legal Ethics and Data Security: Our individual and collective obligation to protect Client data. *Am. J. Trial Advoc.*, *38*, 549.