Project#2: Managers Desk-book

[Author’s name]

[Institute’s name]

Project #2: Managers Desk-book

**Executive Summary**

The aim of developing this desk-book by Chief Information Security Office and Security Team for the company is to appropriately identify potential IT-related problems and offer possible solutions in the form of policies. It is recognized as fundamental guidelines for employees and managers to understand the intensity of IT security risks and offer practical measures. Data Breach Response Policy, Controlling Shadow Policy, and Social Media Policy are considered to propose better solutions to the anticipated data security issues for the company. The idea of Data Breach Policy is helpful to provide mandatory assistance to managers and all the workers when it comes to objectives of proper management of potential hazards of data breaching. Identification of roles, responsibilities, and relevant processes is essential to ensure the successful application of this specific policy.

The applications of Controlling Shadow Policy is also actively associated with proper consideration of all the employees. It is important that the entire IT equipment of the company needs to approved by the IT management department. This perspective is significant to avoid the risk of misuse of the company’s information. Unauthorized use of personal devices and systems by the employees needs to be addressed by offering and implementing Shadow IT policy. Proper documentation of all the procedures and information management system is essential to avoid any hazards of data breaching or improper use of the company’s and client’s sensitive information.

The increasing trend of using social media accounts also requires management of Red Clay Renovations Company to adopt suitable practical measures. Development of proper management of corporate social media account policy is one appropriate practical measure to gain maximum benefits from the instrument of social media. It is critical to share necessary guidelines to all the users on an initial basis to protect the prestige of Red Clay Renovations Company. The overall conduct of employees overall social media platforms should be according to the main vision and relevant objectives of the company. Cooperation and active communication between all the stakeholders is an integral condition to ensure successful execution of all the related policies.

**1st Policy: Data Breach Response Policy**

**Policy Overview:**

Today, business organizations massively facing different challenges related to data protection and proper risk management. The core objectives of cybersecurity policy, comprehensive plan, and programs can never be achieved without the collaboration between different operating departments in case of Red Clay Renovation Corporation. Protection of the client’s data is one major concern that needs to be addressed by adopting appropriate practical measures. The growing risk of data theft in the form of cyber-attacks could be better overcome by implementing data breach response policy. The company is planning to develop the Data Breach Response Policy to ensure clear vision and objectives in the form of risk management. The potential risk of data breaching demands the management of the company to be well prepared by utilizing correct instruments and processes.

**Scope:**

The establishment of this policy relates to all the shareholders who are direct links with the data collection, processing, and handling. The focal practical measures recognized as to collect, evaluate, maintain, dispense, store, use, and proper protection of personally identifiable information or client’s data. The Data Breach Response Policy will explicitly illustrate the aspects under which the policy will be applied considering all the rules and standards of data protection. The governance issues for the company related to the policy perspectives in the forms of mechanisms, feedback, reporting, and implementation.

**Purpose:**

The central objective of this proposed policy is to adopt a systematic procedure to ensure appropriate reporting of all forms of suspected thefts at different governance levels. The possible risks of thefts in the company mainly can be observed in the forms of data, data breaches, or unauthorized access to the data. All the operating units of Red Clay Renovations Corporation must consider the growing risk of data breaching. Increasing the risk of cyber-attacks is the main reason for proposing and enforcing the Data Breach Response Policy.

**Policy Statement:**

The IT Security program of the Red Clay Renovations Company focuses on specific guidelines considering the implications of NIST and the Data Breach Response Policy. The primary aim of this approach is to successfully meet the standards of NIST special publication 800-62, Control Family Incident Response, and the criteria of privacy and security controls established for the company (National Institute of Standards and Technology, 2006).

           It is crucial to develop and establish this policy according to the overall management procedure of Red Clay Renovations Company. Moreover, it is also essential to consider a comprehensive framework for enhancing the approach of improving critical infrastructure cybersecurity within the organization. The identified problem for the company characterized as an information breach that increases the potential risk of stealing clients’ data. Once the risk of data theft reveals, it is crucial to take immediate corrective measures to ensure the protection of aspects of confidentiality and sensitivity of the information.

**Enforcement:**

The proper response to the issue requires the suitable application of the policy considering the core objectives to ensure data protection within the organizational setting. There is a need for considering and implementing different steps to meet the core aim associated with this policy. It is essential to identify the unsatisfactory aspects of the entire information system operating in the organization. It is crucial to consider the proper prevention of data breaches as the essential domain when it comes to the internal policy adopted by the company.

           The human element and technological element are two fundamental prospects that can cause the issue of a data breach for the company. It is crucial to strictly check the performance of these two domains to timely identify potential risks. When it comes to the human aspect, it is essential to provide a necessary guideline to all the workers that they need to ensure data safety and security within the company. Application of additional security actions is required to maintain standards of storing and processing sensitive data under the domain of technical challenge. Complete application of ISO 27001 security principles is obligatory to minimize the hazards of a data breach in an organizational context.

**2nd Policy: Preventing/ Controlling Shadow Policy**

**Policy Overview:**

The practical phenomenon of controlling shadow comprised of some specific protocols. It is an important aspect for the organization’s governance to ensure significantly and desired to handle of shadow IT. The stakeholders need to have the necessary understanding that at which level it is permissible and what restrictions need to be applied. A thorough assessment of IT operations functioning in Red Clay Renovations Company explicitly revealed that there are chances of improper transmission of important organization’s information. It is observed that workers of the company immensely rely on using their technological devices to perform different tasks. This growing trend within an organizational setting ultimately made it integral for Red Clay Renovations Company to properly plan and enforce Controlling Shadow Policy. The increasing security risk in the form of using personal devices by workers can be detrimental for the company to ensure proper data protection (Nieles, Dempsey, & Pillitteri, 2017). All the operating IT system needs to be operating under the company’s information technology system. The inability of this approach can be characterized as one primary risk factor for data security and IT governance within the context of Red Clay Renovations Company.

**Scope:**

The implications of this specific policy are relevant to all the users of the informational technology management system of the company. Proper maintenance of information integrity of the organization is important to successfully deal with issues of misuse of data and potential risk of data loss.

**Purpose:**

The approach of Shadow IT is a potential threat for Red Clay Renovations Company when it comes to the domain of informational and digital security. The organization needs to adopt a set of immediate practical measures to successfully address this concern. The aspects of Shadow IT Policy can be helpful to maintain the efficiency of information technologies used in the company.

**Policy Statement:**

The approach of Shadow IT can bring severe security threat to the company’s overall information technology management system. It is one threatening perspective because it enhances the potential risks of data loss, data breach, and misuse of data for the company. There is a need for establishing significant Controlling Shadow Policy. The spectrum of IT governance of the company needs to be focusing on developing a comprehensive list of various IT procedures, applications, and resources, which are not directly owned by the organization. These programs can be identified in the form of personal devices and applications used by the workers of the company. The potential risks of shadow IT can be mainly observed in the forms of Dropbox, USB, Gmail, Skype, Google Docs, and SD media. All these platforms used by the company’s workers but these can be categorized as major security risks for the company. To successfully cater to this concern, there is a need for offering multiple practical measures under the domain of Controlling Shadow IT policy.

**Enforcement:**

When it comes to practical measures to this policy, then there are multiple options available for the department of management. One of the crucial practical steps for the company is to conduct regular training programs for the workers which are established by the Information Security department of the organization. The second major practical step is to ensure critical and appropriate evaluation of all the services and applications utilized by the company’s workers. Moreover, strict compliance is requiring to scrutinize the overall information technology system of the company. Critical check and balance are also essential when it comes to the assessment of software installation in the workstations under the spectrum of the company’s system management. The active role of the IT security team is required to regularly update all the software and instruments to timely detect any problematic area.

**3rd Policy: Management and Use of Corporate Social Media Accounts Policy**

**Policy Overview:**

The increasing trend of using social media by employees made it essential for the management of Red Clay Renovations Company to develop a proper guiding plan for all the employees. It is necessary for the management to timely indicate all the shareholders when it comes to creating a balance between using social media platforms and organizational work. This specific perspective is a critical practical step to guarantees the overall image of Red Clay Renovations Company. Misrepresentation of the company’s policy is a major issue that can prevail in case of improper use of social media services by the workers. Basic regulations need to consider referring to the approach of proper management of social media services utilized by employees working at different organizational levels.

**Scope:**

The implications of this policy need to be applied to all the workers to develop a proper mechanism of necessary scrutiny within the organizational setting. The role of management is crucial to prepare, develop, and transmit necessary guidelines to all the workers when it comes to using social media within the premises of Red Clay Renovations Company.

**Purpose:**

The main objective of this particular policy is to deliver fundamental guidelines for all the employees concerning the approach of using social media accounts in the company. The perspective of using social media account can be considered as the practical domains of blogs, message boards, chat rooms, newsletters, and other forms of digital applications (Force & Initiative, 2013). The development and application of proper policy are mandatory to meet the objective of data security within the company.

**Policy Statement:**

Establishment of proper policy is a crucial step for the management of the company to protect data security concerning the approach of using social media platforms by the employees. There are some significant instructions or guidelines that need to be shared with all the workers to successfully meet the central objectives of this specific policy. All the employees need to be informed that various corporate social media channels can only be used under the spectrum of Red Clay Renovations Company. Social media under the spectrum of the organization can never be considered for personal in case of all the workers. Assessment of different operations of the company revealed that different forms of social media accounts used mainly for marketing purposes. The management needs to develop a proper plan of actions and necessary guidelines for the workers when it comes to considering social media account for corporate purposes.

**Enforcement:**

It is important to ensure that any information shared on a social media platform never harm the overall reputation of the company. All the representatives of the company need to be vigilant when it comes to approaching potential customers through the instrument of social media. Additionally, it is integral for all the employees to always use secure file sharing programs to avoid any form of misuse of the company’s information (Meister, 2013). All the social media should be completely and strictly controlled by the IT department of Red Clay Renovations Company.

**References**

Force, J. T., & Initiative, T. (2013). Security and privacy controls for federal information systems and organizations. *NIST Special Publication*, *800*(53), 8–13.

Meister, J. (2013). The Future of Work: Why Updating Your Company’s Social Media Policy is Required. Retrieved from:

<https://www.forbes.com/sites/jeannemeister/2013/02/07/the-future-of-work-why-updating-your-companys-social-media-policy-is-required/#5b77793e230d>

National Institute of Standards and Technology. (2006). Information Security Handbook: A Guide for Managers. Retrieved from:

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf>

Nieles, M., Dempsey, K., & Pillitteri, V. (2017). *An introduction to information security*. National Institute of Standards and Technology.