Unit assignment

This could include: tailoring requirements to be suitable for particular roles within he organization for which persons are considered; ensuring that persons fully understand the security responsibilities and liabilities of their role(s); ensuring awareness of information security threats and concerns, and the necessary steps to mitigate those threats; and Providing all persons to support organizational privacy and security policies in the course of their normal work, through appropriate training and awareness programs that reduce human error; and ensuring that persons exit the organization, or change employment responsibilities within the organization, in an orderly manner.

Roles and susceptibilities Security roles and responsibilities of employees, contractors and third-party users should be defined and documented in accordance with the organization’s information privacy and security policies. This could include: To act in accordance with the organization’s policies, including execution of all processes or activities particular to the individual’s role(s); To protect all information assets from unauthorized access, use, modification, disclosure, destruction or interference; To report security events, potential events, or other risks to the organization and its assets Assignment of responsibility to individuals or actions taken or, where appropriate, responsibility for actions not taken, along with appropriate sanctions formal. Procedures and policies To be implementing in any IT domain controls by the organization.

Proper password security Properly managing log files Secure firewall rule sets Handle security incidents Secure data classifications Limited employee access dangerous websites Terms and conditions of employment Employees,

contractors, and third party users should agree to and sign a statement of rights and responsibilities for their affiliation with the organization, including rights and responsibilities with respect o information privacy and security. This statement could include specification of: the scope of access and other privileges the person will have, with respect to the organization’s information and information processing facilities; The person’s responsibilities, under legal-regulatory-certification requirements and organizational policies, specified in that or other signed agreements. Responsibilities for classification of information and management of organizational information facilities that the person may use.

Procedures for handling sensitive information, both internal to the organization and that achieved from or transferred to outside parties. Responsibilities that extend outside the organization’s boundaries (e. G. , for mobile devices, remote access connections and equipment owner by the organization. The organization’s responsibilities for handing of information related to the person him/herself, generated in the course of an employment, contractor or other third party relationship. An organizational code of conduct or code of ethics to the employee, contractor or third party. Actions that can be anticipated, under the organization’s disciplinary process, as a consequence of failure to observe security requirements.