Unit assignment

This could include: *tailoring requirements to be suitable for particular roles within the 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 responsibilities 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, attention events, or other risks to the organization and its assets * Assignment of responsibility to individuals for 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 * Easily accessible network flow diagrams * Secure firewall rule sets * Handle security incidents * Secure data classifications *

Limited employee access dangerous websites Policies that will accepted by the organization and needs to be implementing ASAP.

Acceptable Use Policy I I Password Policy I Backup Policy I I Network Access Policy I Incident Response Policy I Remote Access Policy I Virtual Private Network (VPN) Policy I I Guest Access Policy I Wireless Policy I I Third Party Connection Policy I Network Security Policy I I Encryption Policy I Confidential Data Policy I I Data Classification Policy I Mobile Device Policy I Retention Policy I Outsourcing Policy I I Physical Security Policy I E-mail Policy I I I Terms and conditions of employment Employees, contractors, and third party users should agree to and sign a statement of rights and responsibilities or their affiliation with the organization, including rights and responsibilities with respect to 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 received 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.

Additional pre-employment agreements Where appropriate, employees, contractors and third-party users should be required to sign, prior to being given access or other privileges to information or information processing facilities, additional: * confidentiality or non-disclosure agreements (see Confidentiality agreements); and/or * Acceptable use of assets agreements. Management responsibilities Management should require employees, annotators and third party users to apply security controls in accordance with established policies and procedures of the organization. This could include: * appropriately informing all employees, contractors and third party users of their information security roles and responsibilities, prior to granting access to sensitive information or information systems using Terms and conditions of employment. Providing all employees, contractors and third parties with guidelines/rules that state the security expectations of their roles within the organization; * achieving an appropriate level of awareness of security controls mongo all employees, contractors and third parties, relevant to their roles and responsibilities, * achieving an appropriate level of skills and qualifications, sufficient to execute those security controls; * assuring conformity to the terms and conditions of employment related to privacy and security; * motivating adherence to the privacy and security policies of the organization, such as with an appropriate sanctions policy; and * Mitigating the risks of a failure to adhere to policies, by ensuring that

all persons have appropriately-limited access to the organization’s information and information facilities (see Authentication and access control).

Information security awareness, education and training All employees of the organization, and, where relevant, contractors and third party users, should receive appropriate awareness training in and regular updates of organizational policies and procedures relevant to their job functions. This could include: * A formal training process that includes information privacy and security training, prior to being granted access to information or information systems. * Ongoing training in security control requirements, legal-regulatory- ratification responsibilities, and generally accepted security procedures, suitable to the person’s rules and responsibilities. Disciplinary process There should be a formal disciplinary process for employees who have committed a security breach. This could include requirements for: * appropriate evidentially standards to initiate investigations (e. G. “ reasonable suspicion” that a breach has o c Cue r red); appropriate investigatory processes, including specification of roles and responsibilities, standards for collection of evidence and chain of custody f evidence; * disciplinary proceedings that observe reasonable requirements for due process and quality of evidence; * reasonable evidentially and burden- of-proof standards to determine fault, that ensure correct and fair treatment for persons suspected of a breach; and * sanctions that appropriately take into consideration factors such as the nature and gravity of the breach, its impact on operations, whether it is a first or repeat offense, whether or not the violator was appropriately trained, whether or not the violator exercised due

care or exhibited negligence. Termination responsibilities Responsibilities and practices for performing employment termination or change of employment should be clearly defined and assigned.

This could include: * termination processes that ensure removal of access to all information resources (see also Removal of access rights); * changes of responsibilities and duties within the organization processed as a termination (of the old position) and re-hire (to the new position), using standard controls for those processes unless otherwise indicated; * processes ensuring that other employees, contractors and third parties are appropriately informed f a person’s changed status; and any post-employment responsibilities are specified in the terms and conditions of employment, or a contractor’s or third party’s contract. Return of assets All employees, contractors and third parties should return all of the organization’s information and physical assets in their possession upon termination of the employment relationship or contract.