**QUESTIONNAIRE ON PROTECT**

**SOHAIL MOHAMMED**

**Controls:**

1. Identity Management, Authentication and Access Control (PR.AC)

2. Awareness and Training (PR.AT)

**1.Does the organization has a centralized repository to keep all the user identity information ?**

Maintaining a central repository of all the user information will help the organization run and maintain operations smoothly, such as at the time of data breach or user losing their credentials. Upon request they can be searched and recovered from the central repository. This also helps in linking the different user information together.

**2.Does the organization have any access restrictions for the employees who access and manage the data and assets of the company ?**

Having access restrictions is a must for any company. Each employee should be given access only to the data and assets that he or she is working on. If there are no access restrictions and anyone can access anything there are more chances of data brokers selling the companies data to other who can benefit from it.

**3.What level of authentication is used to verify the users and devices connected to the organization ?**

Different organizations require different types of authentication methods. Deciding which methods is suitable and more secure is the task. Should it be U2F security token or mobile passcode or just an otp message. Adding extra layers of security is always better because of the increasing authentication breaches

**4.DO you use any encryption/decryption techniques for identity and credential verification ?**

While authentication technique being more flexible than encryption methods, Encryption helps in transferring important data or messages more securely. Data is the most vulnerable while transferring encryption/decryption helps protect data integrity and privacy while it is transferred between two or more devices

**5.Is the user made aware of the use of his encryption key and on security issues when shared with others ?**

While performing encryption a key is generated to decrypt the data transferred. It could be a public key or private key. User should be made aware that the encryption key only belongs to him and not to be shared with others, user should know the repercussions on sharing it with others.

**6.Did your organization implement any policies for remote access of the company’s data and information ?**

Remote access has grown rapidly in recent times, people connect to organizations resources being at home, office or elsewhere. Technology is not confined with in the organization’s physical walls. This remote access brings is many issues like connectivity, information security etc. Hence organizations should have certain rules and policies to access its business’s network.

**7.Does the organization keeps track of user, device logins and is the user made aware of this ?**

Keeping the user login information helps us keep track of the user patterns detect any malicious activity. User must be asked to authenticate the devices which he or she regularly uses for access. If someone logs in with a new device user should be notified about it. This helps restriction of using non-authorized devices.

**8.Is the access mechanism associated with the privileges that employees are given ?**

Before giving access to the organizations data or assets to the employee the access mechanism should evaluate the privileges of that to make sure that the employee is qualified enough to access it. This will prevent important data and assets falling to wrong hands. And any misuse should be notified to the higher authorities.

**9.Is every user given a unique identification number to solve conflicting names problem ?**

For a large organization it is very common for different users to have a common first or last name. The name is generally used to create the login credentials. How is the company willing to handle this situation. By giving each user a unique ID ? or making a unique key out of the given name ? or something else. We need to decide which suits our organization best.

**10.Are the employees given enough training before actually entering the designated job ?**

Even when the employees are qualified enough to work for our organization they require certain amount of training before actually starting the job to get familiar with the work environments and methods. How many months of training is given and at what levels. Who are the employees trained under ?

**11.Is there any evaluation done for assigning of the privileges of employees ?**

After the training is commenced each employee needs to be assigned privileges based on their qualification, experience, designation assigned etc. What criteria does our organization use to assign privileges to them and who decides it. Miscalculation of this can lead to major issues like employee not able to handle the tasks given.

**12.Are the employees well aware of the privileges they are given and what measures are taken when they exploit their privileges ?**

Each employee should know what they can and cannot access, this should be made clear during their training program. A higher authority should be present to decide what happens when an employee tries to access system that is above the privileges given to them. Moreover, what are the precautions taken by our organization to prevent these situations.

**13.Do the third-party stakeholders have the privilege to access and modify the internal data or information of the company ?**

Third-party stake holders are also an integral part for running of a company, but how much importance is given to them. Are they allowed to access or modify the company’s internal data. Do they have any special privileges that give them right to access it. These doubts should be made clear before making any agreements with them.

**14.To what extent does the cybersecurity personnel acknowledge the data integrity policies of the organization ?**

The information security officer working in the company should be aware of what type of data he or she is trying to protect and importance of it. He should know the sensitivity, rules and regulations associated with the company’s data. The policies should right fit the type of organization and data it is protecting.

**ANGELA BHAGATH**

**Controls:**

1. Data Security (PR.DS)
2. Protective Technology (PR.PT)
3. **Do you collect/process personal data of your customers, employees or any other third party?**

*‘Personal data’ means information which identifies any living individual or can, with other information held by you, identify any individual. ‘Processing’ of personal data means obtaining, recording or holding the information. As a business, you will be handling the personal information of your employees, suppliers and / or customers: it is therefore likely that your activities will be caught by the provisions of the DPA (Data Protection Act).*

Dropdown for Yes/No

1. **Do you have a Policy on data protection in your organisation?**

*You should establish a data protection policy in your business to ensure your legal obligations are met. The policy should take into account the particular personal data needs of the business as well as the way it processes this information. The policy should also address areas where personal and sensitive data might inadvertently leak.*

Dropdown for Yes/No

1. **Do security controls or procedures include measures to facilitate the use of encryption?**

*Encryption is important in many circumstances to ensure that information is stored in a form that cannot be easily understood by unauthorised individuals or entities. Encryption methods should be reviewed regularly to ensure they continue to be relevant and effective and are used where necessary. This includes ensuring that the scope of encryption is wide enough so that attackers cannot access another unencrypted copy of your encrypted information.*

Dropdown for Yes/No

1. **What kind of backup solution does your organization use?**

*To prevent the information you hold from being lost, you should make copies of important files and store them on a physical device or online using a cloud-based storage solution.*

1. **Do security controls or procedures include measures to invoke a business continuity/disaster recovery plan?**

*In the event of a data breach, having a response plan that includes procedures and clear lines of authority can assist you to contain the breach and manage your response. Ensuring that staff (including contractors) are aware of the plan and understand the importance of reporting breaches is essential for the plan to be effective.*

Dropdown for Yes/No

1. **How often does your organization perform a test data recovery from backups to verify integrity?**

*Frequent tests and test results should ensure that the technologies and procedures in question backed information up successfully, restored it successfully, and that the backup targeted and captured all the data that should be backed up. Along with the frequency of testing, the quality of testing counts as well.*

1. **Is data saved to unauthorised storage locations such as USB sticks?**

*You need to guard against internal threats such as unauthorised access or misuse of personal information by your staff, including contractors (the trusted insider risk). Trusted insider breaches can occur when staff mishandle personal information while carrying out their normal duties. Limiting such access is an important personal information security mechanism.*

Dropdown for Yes/No

1. **Are there audit trials in place recording the identity of operators entering, changing, confirming or deleting data?**

*Unauthorised access of personal information can be detected by reviewing a record of system activities, such as an audit log. Maintaining a chronological record of system activities (by both internal and external users) is often the best way for reviewing activity on a computer system to detect and investigate privacy incidents. Audit logs should also be named using a clear naming convention.*

Dropdown for Yes/No

1. **Do users that can access devices that store or process sensitive information have a unique user name and complex password to access the system?**

*Appropriate authentication can be used to limit a person’s access both to the system or network and also to the information contained within it. It can also assist in mitigating security risks such as ‘social engineering’.*

Dropdown for Yes/No

1. **Is the production network segmented in to different zones based on security levels?**

*Segregating an entity’s network into multiple functional segments makes it difficult for an intruder to propagate inside the network. Proper network segmentation assists in the creation and maintenance of network access control lists. Segmentation can also allow for different security measures to be applied to different types of information depending on its sensitivity and the risks associated with it.*

Dropdown for Yes/No

1. **What types of security reviews does the organization perform on outsourced software?**

*Removing or disabling unneeded software, operating system components and functionality from a system reduces its vulnerability to attack, and can make it harder for malware to run or an attacker to gain access.*

1. **Do you have policies, procedures and resources in place to determine whether personal information you hold needs to be: retained, destroyed or de-identified?**

*Where an entity holds personal information it no longer needs for a purpose that is permitted under the APPs (Australian Privacy Principle), it must ensure that it takes reasonable steps to destroy or de-identify the personal information (APP 11.2).*

Dropdown for Yes/No

1. **Are all endpoint laptops that connect directly to production networks centrally managed?**

*Endpoint security systems work on a client/server model in which a centrally managed server or gateway hosts the security program and an accompanying client program is installed on each network device. When a client attempts to log onto the network, the server program validates user credentials and scans the device to make sure that it complies with defined corporate security policies before allowing access to the network.*

Dropdown for Yes/No

**PAVINDRA REDDY PONDUGALA**

**Controls:**

1. Information Protection processes and Procedures (PR. IP)
2. Maintenance (PR.MA)

Q1. **Does the organisation have a baseline configuration of Information System which is documented?**

Justification:

*Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components, network topology, and the logical placement of those components within the system architecture. Baseline configurations of information systems reflect the current enterprise architecture.*

Drop Down Box: Yes/No

**Q2. Is the baseline Configuration of information System Reviewed and Updated Frequently according to the organisation-defined frequency?**

Justification:

*Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. Reviewing the configuration helps the organisation to know the status of the Systems. Each organisation defines the frequency for the review depending upon their systems, network, software and hardware’s they use. Performing the review helps the organisation to be updated with its configuration.*

Drop Down Box: Yes/No

**Q3. Does the organisation maintain an automated mechanism to maintain baseline Configuration of Information System?**

Justification:

*Automated mechanisms that help organizations maintain consistent baseline configurations for information systems include, for example, hardware and software inventory tools, configuration management tools, and network management tools. Such tools can be deployed and/or allocated as common controls, at the information system level, or at the operating system or component level (e.g., on workstations, servers, notebook computers, network components, or mobile devices).*

Drop Down Box: Yes/No

Q4. **Does the organisation retain previous versions of baseline Configurations of the Information Systems to support rollback?**

Justification:

Retaining previous versions of baseline configurations to support rollback may include, for example, hardware, software, firmware, configuration files, and configuration records. In case of any attack or loss of some basic information, maintain previous versions can help organisations to have a good idea about the configuration of Information System.

Drop Down Box: Yes/No

Q5. **Does the organisation consist of automated mechanisms to document and notify the approval authorities regarding changes to information Systems?**

Justification:

*Changes to information systems include modifications to hardware, software, or firmware components and configuration settings. Documenting these can help the organisation for future reference and further developments. Typical processes for managing configuration changes to information systems include, for example, Configuration Control Boards that approve proposed changes to systems.*

Drop Down Box: Yes/No

Q6. **Does the organisation Analyse the changes to information System in separate test environment before implementation?**

Justification:

*Separate test environment in this context means an environment that is physically or logically isolated and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment, and information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means.*

Drop Down Box: Yes/No

Q7. **Does the organisation have access restriction for change to the information system?**

Justification:

*Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. Organizations permit only qualified and authorized individuals to access information systems for purposes of initiating changes, including upgrades and modifications. They maintain records of access to ensure that configuration change control is implemented.*

Drop Down Box: Yes/No

Q8. **Does the organisation have defined the software Blacklisting and Whitelisting that are executed on the Information System?**

Justification:

*The process used to identify software programs that are not authorized to execute on organizational information systems is commonly referred to as blacklisting. Organizations can implement, instead of this control enhancement if whitelisting (the stronger of the two policies) is the preferred approach for restricting software program execution. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.*

Drop Down Box: Yes/No

Q9. **Does the organisation have the capability of shutting of power to the information System during emergency situations?**

Justification:

*During emergency situations shutting of power to the information Systems can protect the system from unauthorised activation. These may include data centres, server rooms and mainframe computer rooms.*

Drop Down Box: Yes/No

Q10. Does your organisation have the Security planning Policy Dealing with DEFENSE-IN-DEPTH and SUPPLIER DIVERSITY?

Justification:

*Organizations strategically allocate security safeguards (procedural, technical, or both) in the security architecture so that adversaries must overcome multiple safeguards to achieve their objective. Requiring adversaries to defeat multiple mechanisms makes it more difficult to successfully attack critical information resources and also increases the likelihood of detection. Placement of security safeguards is a key activity. Different information technology products have different strengths and weaknesses.*

Drop Down Box: Yes/No

Q11. **Does your organisation have the Systems and services security policy?**

Justification:

*This policy develops, documents, and disseminates to [organization-defined personnel or roles]. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.*

*Reviews and updates the current:*

*1. System and services acquisition policy [organization-defined frequency]; and*

*2. System and services acquisition procedures [organization-defined frequency].*

Drop Down Box: Yes/No

Q12. **Is the Attack surface Reviews performed by Information System?**

Justification:

*Attack surfaces of information systems are exposed areas, that make those systems more vulnerable to cyber-attacks. This includes any accessible areas where weaknesses or deficiencies in information systems (including the hardware, software, and firmware components) provide opportunities for adversaries to exploit vulnerabilities. Attack surface reviews ensure that developers: (i) analyze both design and implementation changes to information systems; and (ii) mitigate attack vectors generated as a result of the changes.*

Drop Down Box: Yes/No

Q13. **Does the organisation Sanitize the information System media before disposal?**

Justification:

*The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization.*

Drop Down Box: Yes/No

Q14. **Does your Information System policy employ automated mechanism for controlled maintenance?**

Justification:

*The automated mechanism produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.*

Drop Down Box: Yes/No

Q15. Does your organisation Inspect tools, Media and prevent unauthorised removal?

Justification:

*Inspection of maintenance tools, organizations determine that the tools have been modified in an improper/unauthorized manner or contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling. Inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with organizational incident handling policies and procedures.*

Drop Down Box: Yes/No