**8.1.1 Assigning all users a unique ID before allowing them to access system components or cardholder data**

Companies that accept or use credit debit cards are required to comply with the PCI DSS requirements. One of these requirements is to identify and authenticate access to system components. This specific requirement is part of the goal of the standard, which involves implementing strong access control measures. The concept of identifying and authenticating access to system components involves establishing a unique ID for each person to ensure that employees are accountable for their actions. This technique allows operations performed on sensitive data to be traced back to a known authorized person and process.

In order to ensure the assigning all users a unique ID component of the requirement, several technological and policy tactics can be used in combination. Technical controls should be designed in a way that they can ensure each user is uniquely identified instead of using one ID for several employees. This mechanism allows organizations to maintain individual responsibility for actions and an effective audit trail per employee. It will also help resolve issues when a misuse or malicious intent occurs. Technical tactics should also involve proper controls in identification, authentication, and authorization phases. Once an employee enters their ID or username, the system must properly verify that the user is whom they say they are. Then, the user authenticates (proves that they are whom they say they are) by entering a password. Other forms of authentication are better than this traditional method. These include using smart cards, RSA token, and biometrics (thumbprint, retina scan, and so on). After that, systems must grant proper authorization based on the need to know and the principle of least privilege to allow employees access to sensitive card data.

Policy tactics that ensure the PCI DSS requirement to Identify and authenticate access to system components should involve identity and access management policy. This policy should describe the types of electronic identities in use for systems and applications; criteria for creating identities and accounts; how identities should be authenticated; how authorizations should be managed, and how accounts and privileges should be deployed. The scope of such a policy should include the responsibilities of individual employees, such as password policies and the duties of the IT staff or others that provide access to the stored data. They are in charge of properly configuring the different types of user accounts, authentication methods, and proper authorization (role-based authorization, for example) based on least privilege and separation of duties. They should also be responsible for auditing employees’ activities to ensure everything works as designed and identify any malicious intent.

References

Ballad, B., Banks, E, K., Chapple, M., Ballad, B. (2017). *Access Control, Authentication, and Public Key Infrastructure, Second Edition.* Burlington, MA. Jones & Bartlett Learning.

Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures. (2018). Retrieved from https://www.pcisecuritystandards.org/documents/PCI\_DSS\_v3-2-1.pdf?agreement=true&time=1568474549174