VISA Europe
Default & Shared Credentials

To simplify deployment, many device manufacturers and software providers supply products which are configured with default username and passwords. Unfortunately, many organisations are failing to perform basic security checks prior to deploying a new device or installing a new application. If a device is deployed, or an application installed without first disabling unnecessary accounts and changing default passwords, an organisation places itself at serious risk of a data breach. Default user accounts and passwords are often published on the Internet and many hackers actively make use of this information to gain illegal access to systems.

Using default credentials is much like buying an expensive new lock for your front door and then providing copies of the key to the global criminal community. Once through the front door, hackers can begin the process of escalating their attack and cause massive financial and reputational damage to your organisation.

"Using default credentials is much like buying an expensive new lock for your front door and then providing copies of the key to the global criminal community."

Mitigating Techniques

Proper management of user accounts and passwords form a valuable barrier in defending any system against a data breach. Diligently following the simple guidance below will help make your organisation considerably more secure. Please note that many of these controls should be implemented in conjunction with each other (rather than in isolation) to form a layered approach to system defence.

Change Default Passwords	Prior to placing any device or application into production, the first action that an organisation must take is to change/disable all default accounts and passwords. If you are unsure how to change default accounts or passwords, you should consult the supplied manuals for the device/application in question and/or contact your supplier for guidance. For devices and applications that have already been deployed, you should immediately investigate which systems are using default credentials and change them at the earliest possible opportunity.
Use Complex Passwords	Changing a password by itself may not be sufficient if the replacement password is "weak". A weak password is one which is relatively trivial for a hacker to guess. For example, a word from a dictionary would be considered a weak password. You should look to use passwords that are at least 7 characters long and use a combination of uppercase and lowercase alphabetic characters, numbers and special characters (e.g. !"£$%^) when creating a password.
Remove Inactive Accounts	Accounts that are no longer in use should be disabled. If an employee leaves your organisation, you should disable his or her account immediately.
Don't Share Credentials	Shared credentials are much like a master key, unless absolutely necessary you should not use the same account details across multiple systems or share account details between multiple users. If a 3rd party is responsible for managing any of your systems, you should verify with them that the account details used to manage your systems are unique to your organisation and not reused by the 3rd party across multiple clients.
Change Passwords Frequently	User passwords should be changed at least once every three months.
Monitor for Suspicious Activity	Monitoring for unauthorised access to systems should be performed as an ongoing concern. For example, access attempts by an employee outside of their scheduled work hours or multiple failed login attempts should be investigated as it may indicate an attack against your system.
Additional Controls	
Limit Number of Incorrect Password Attempts	If the device or application supports the ability to lock an account after a number of incorrect password attempts, then this feature should be enabled. If you are unsure if your device or application supports this feature or how to enable it, you should consult the supplied manuals for the device/application in question and/or contact your supplier for guidance.
Use The Least Privilege Possible	If a user does not require access to a system or application to perform their role then by default they should be excluded from accessing it. A user should only be allowed the minimum privileges necessary to perform their job.

Appendix A – Additional Resources

Microsoft

- Provides a tool to check the strength of passwords – http://www.microsoft.com/protect/fraud/passwords/checker.aspx
- Provides a guide on creating strong passwords – http://www.microsoft.com/uk/protect/yourself/password/create.mspx