DCX Technology ("DCX") - Information Security and Anti Money Laundering (AML) Policy

Last update 7th March 2024

DCX is committed to managing business risk and ensuring an environment, which protects DCX information and information resources from accidental or intentional unauthorized use, modification, disclosure, or destruction. Adherence to DCX information security policies is necessary to achieve organizational security objectives of safeguarding the confidentiality, integrity, and availability of DCX information and information assets.

The intent of the Information Security Policies, Procedures, Standards, and Guidelines is to:

- Establish an information policy management and governance structure applicable across DCX platforms.
- Address all the requirements of the Payment Card Industry (PCI) Data Security Standard (DSS) version 4 (or more current version if applicable).
- Comply with applicable regulatory requirements.
- Ensure employee, contractor, and business partners understanding and acceptance of organizational requirements for protecting DCX information resources.
- Protect customer and employee information from unauthorized use, disclosure, modification, or destruction.
- Clarify management, employee, and external business associate responsibilities and duties with respect to the protection of information resources.
- Standardize security controls across the enterprise and coordinate the security efforts throughout DCX.
- Enable management, employees, and external business employees to make information security decisions in accordance with approved information security policies.

DCX is also bound by Australian law to take steps to ensure that it is not involved in the facilitation of money laundering or terrorist financing.

Various AML measures are in place designed to articulate our commitment to detecting, preventing and reporting attempts to use our financial services platform to launder money, to finance illegal activities such as terrorism and drug trafficking, or to commit fraud.

The following is a list of some of these measures:

- All clients must undergo a verification check to confirm identity before being allowed to work with DCX.
- Fiat currency withdrawals can only be made to a bank account held in the same name as the name of the customer that performed the KYC. The allowed exemptions are where there are joint accounts, or the account holder is the main signatory of the account.
- Fiat currency deposits can only be accepted from a bank account held in the same name as the name of the customer that performed the KYC. The allowed exemptions are where there are joint accounts, or the account holder is the main signatory of the account.
- DCX is obliged to report any suspicious activity to the relevant authorities.
- Cryptocurrency withdrawals or deposits may require the address to be white listed by confirming a small transfer to the address in question. The confirmation is required when the amount exceed the limits requiring enhanced due diligence.