MFSA
MALTA FINANCIAL SERVICES AUTHORITY

Guidance Notes on Cybersecurity

Contents

Chapter 1

Introduction

1 Introduction

While technology innovation is ever-increasing, it also provides new opportunities for cybercrime. The Authority has identified the need to ensure that the industry operating within the Distributed Ledger Technology ('DLT') sphere implements the necessary cybersecurity solutions in order to effectively mitigate the cyber threats present, in view of the inherent risks of this sector.

The Authority is thus proposing these Cybersecurity Guidance Notes, which are applicable to those persons specified in Guidance Note 2.1.1, as a minimum set of best practices and risk management procedures to be followed in order to effectively mitigate cyber risks.

Chapter 2

Guidance Notes

2 Guidance Notes

2.1 Scope and Applicability

2.1.1 The [i] Supplementary Conditions applicable to Professional Investor Funds investing in Virtual Currencies, under Section 9 of Appendix I to Part B of the Investment Services Rules for Professional Investor Funds (link) and [ii] the Virtual Financial Assets Rulebook (collectively (i) and (ii) - the 'Rulebooks') require the decision-making body of a person regulated thereunder (the 'Entity') to establish and maintain a prudent operational governance framework. The framework should contain provisions relating to, *inter alia*, cybersecurity.

2.1.2 The decision-making body, as mentioned in Guidance Note 2.1.1 above, shall refer to the following:

i. Governing Body of Professional Investor Funds investing in Virtual Currencies;
ii. Board of Administration of VFA Agents;
iii. Board of Administration of Issuers; and
iv. Board of Administration of VFA Service Providers.

2.1.3 The Entity's cybersecurity architecture shall comply with internationally and nationally recognised cybersecurity standards, as applicable, and shall, *inter alia*, be in line with the provisions of:

i. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ('GDPR');
ii. Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC ('PSD2');
iii. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ('NIS');
iv. Any applicable EU legislation as may be transposed into national legislation; and
v. Any other relevant legislation which may have regulatory implications on the Entities.

2.1.4 Despite the fact that these Guidance Notes refer predominantly to the term "cybersecurity", it is imperative that a cybersecurity architecture of an Entity embraces holistic data security, i.e. network and information security, and should cover management of data in any format, (including digital, physical, audio-visual, etc.) and in any state (including in-transit and at-rest).

2.1.5 These Guidance Notes are not intended to be comprehensive or to replace any provisions of the Rulebooks, and shall be seen in conjunction with internationally and nationally recognised cybersecurity standards, as applicable. These Guidance Notes are also without prejudice to any additional requirements applicable to Entities emanating from the Innovative Technology Arrangements and Services Act (Chapter 592 of the Laws of Malta), regulations made, rules or guidelines issued thereunder or any other applicable legislation. Their purpose is to guide the industry vis-à-vis the establishment, implementation, and monitoring of cybersecurity. Entities are expected to conform to these Guidance Notes in order to ensure proper management of cybersecurity for the benefit of the Entity itself, any stakeholders and the unit holders involved.

2.1.6 These Guidance Notes reflect the Authority's approach towards effective management of risks and the understanding of risk factors directly linked to an Entity's operation in the financial services landscape. In recent years, a number of initiatives at international level focused on establishing

regulatory frameworks governing the cybersecurity requirements of various actors across the financial industry, including *inter alia*:

i. European Banking Authority's (EBA) Guidelines on Internet Payments Security;
ii. EBA's Guidelines on the assessment of the Information and Communication Technology (ICT) risk; and
iii. EBA Guidelines on Security Measures for Operational and Security Risks under the PSD2.

2.1.7 A number of cybersecurity standards implemented at international or national level, often driven by industry-specific needs, provide a basis for cybersecurity strategies proportionate to the changing threat landscape. This rise in initiatives relating to cybersecurity is imminently confronted with ever-more sophisticated cyber-attacks driven by various threat agents.

2.1.8 These Guidance Notes are based on a mapping exercise involving a number of recognised cybersecurity standards and guidance, including *inter alia*:

i. ISO/IEC 27k (in particular 27001, 27002, 27005, 27014, 27017 and 27018);
ii. ISO 31000;
iii. US NIST Cybersecurity Workforce Framework;
iv. CPMI-IOSCO Guidance on cybersecurity;
v. PCI-DSS;
vi. ISACA/ COBIT 5; and
vii. CryptoCurrency Security Standard ('CCSS').

2.1.9 Notwithstanding the fact that the scope of GDPR goes significantly beyond the area of cybersecurity, these Guidance Notes shall be read in conjunction with the provisions of GDPR if the Entity in question is collecting or processing personal data.

2.1.10 The Entity should make reasonable and proportionate investment in cybersecurity tools (and information security systems in general) and supplementary knowledge, and should establish cybersecurity policies and procedures at the development/ start-up stage.

2.1.11 The Authority may update or amend these Guidance Notes from time to time as it deems necessary. Moreover, the Authority reserves the right to conduct, in the future, an exercise aiming at assessing Entities' levels of cybersecurity.

2.2 Who are these Guidance Notes addressed to?

2.2.1 As a general rule, the decision-making body, as further specified in Guidance Note 2.1.2, is primarily responsible for the establishment and maintenance of appropriate governance structures, good conduct and suitable risk management policies of an Entity.

2.2.2 This notwithstanding, each Entity should designate a person responsible for establishing, maintaining and overseeing the internal cybersecurity architecture, who should be appointed to act as Security Officer, Chief Security Officer, Chief Information Security Officer or any other designation (the 'CISO'). Having the same authority, function and responsibility, this person should be promoting a corporate culture focused on an active approach to cybersecurity education and training to be undertaken by any member of the decision-making body, member of staff, contractual worker and/or service provider, as reasonable. Entities should ensure that the CISO position is only accepted by individuals who fully understand the extent of responsibilities attached to the role and who are duly qualified and competent, possessing sufficient knowledge, professional expertise and experience, to fulfil such role.

2.3 Methodology

2.3.1 Each of the below Guidance Notes should be viewed from three different aspects, namely (i) People, (ii) Processes and (iii) Technology. The involvement of, and impact on, all three aspects shall be given equal importance in terms of investment and should be monitored on an on-going basis and updated, or upgraded, as necessary.

2.3.2 Any activity or action taken by the CISO should address risks relating to management of data in any format (including digital, physical, audio-visual, etc.) and in any state (including in-transit and at-rest). Management of data includes in particular, but not exclusively, input, transfer, storage, reproduction, recycling and disposal/ sanitisation of data. Data management shall be based on adequate Data Governance, Data Quality and Data Architecture models and shall be given equal importance at various operational levels of cybersecurity architecture including: Governance, Identification, Protection, Detection, Response and Recovery.

Without prejudice to the generality of the foregoing, the CISO's responsibilities should include, *inter alia*, the following:

i. Overall integration of cyber defence management aspects within the Entity;
ii. Advise senior management on cyber defence management;
iii. Assist management in formulation and implementation of cyber defence policy;
iv. Establish a corporate methodology for cyber risk management;
v. Develop, oversee implementation, and monitor a comprehensive and in-depth cyber risk management program;
vi. Define detailed policies and working procedures for the implementation of cyber defence controls;
vii. Promote cyber threats awareness and provide training on mitigation processes across the Entity including employees, suppliers, partners and customers;
viii. Work with the relevant functions (technological and business) within the Entity in order to analyse and assess the levels of inherent risk, the respective controls required, and the levels of residual risk and exposure to cyber threats;
ix. Coordinate and liaise with third parties on cyber defence matters;
x. Develop relevant metrics and measurements, prepare and disseminate status reports and provisioning of continuous reports;
xi. Integrate and monitor cyber incident response management within the Entity;
xii. Initiate and execute cyber exercises;
xiii. Lead and coordinate cyber defence management processes; and
xiv. Undertake cyber defence control assessment.

2.3.3 Each Entity should establish a cybersecurity architecture, the quality and compliance of which should be examined by means of self-assessment.

The self-assessment should examine the probability of a cyber-attack (and other threats affecting the Entity's cybersecurity) and the impact or magnitude of such attack on the Entity. The CISO should determine weakest links within the Entity and its surroundings and shall perform a cost-benefit analysis of aspects relating to the cybersecurity architecture.

For the purpose of this self-assessment, the CISO should assess the Entity's cyber risk appetite and its capabilities, strong and weak points on all three aspects mentioned in Guidance Note 2.3.1.

2.3.4 In order to manage possible threats, the Entity should consider various threat scenarios to determine its state of security and have adequate 'situational awareness' to differentiate between normal and abnormal/irregular activities.

2.3.5 The Entity's cybersecurity architecture shall be based on, or at least take into account, internationally and/or nationally recognised standards on cybersecurity and related risk and data management requirements.

2.4 Organisational Governance

2.4.1 Each Entity should establish a Cybersecurity Framework ('CSF') taking into account its specific set-up, nature of business, contractual agreements and human resources arrangements. The CSF should be [i] in writing, [ii] approved by the decision-making body and [iii] include, *inter alia*, the following:

i. Information and data security roles and responsibilities, including the designation of the CISO;
ii. Privileged access management policy;
iii. Sensitive data management policy;
iv. Threats management policy;
v. Security education and training
vi. Ongoing monitoring policy;
vii. Risk assessment, the frequency and extent of which should be determined by the Entity;
viii. Maintenance of audit trails to detect and respond to Cybersecurity events;
ix. Establishment of an incident response and recovery plan;
x. Establishment of business continuity plan; and
xi. Establishment of security policy for third party service providers.

In relation to point (vi) above, Entities should have in place the necessary systems that continuously monitor their networks in real-time with intrusion detection measures to prompt alerts of any cyber threats. These security systems should be fine-tuned in a way that categorises cyber threats and prioritises them. These should also be analysed and tested regularly to calibrate and improve the detection process. Where these systems are outsourced, Entities should ensure that the third party service provider actively monitors the networks and that any anomalous or suspicious activity is immediately reported to the Entities for further investigation.

In relation to point (vii) above, Entities are expected to conduct a risk assessment and draw up a report attesting to the mitigating measures that have been, or will be, put in place to safeguard against the risks identified in the said risk assessment. This report shall further include any findings emanating from the ongoing monitoring conducted pursuant to point (vi) above in relation to these Entities, including inter alia the outcome/s of any threat hunting, vulnerability assessment/s and/or penetration testing/s. Copies of the said risk assessment and report should be held at the Entity's registered address and made available to the Authority upon request.

2.4.2 In terms of roles and responsibilities, the CSF should define persons, processes and means of entering into and maintenance of contact with: (a) national authorities, (b) special interest groups, and/or where and if applicable, (c) media. It should also define hierarchy of internal communication in relation to any aspects concerning cybersecurity.

2.4.3 The CSF should include provisions relating to control and change management. Control management should empower the CISO, with preventive, detective and corrective control powers enabling controls to be conducted on a regular basis. Change management should cover areas such as human resources, supply chain and technical, regulatory and legal developments.

2.4.4 Based on the CSF, any Entity should establish a Business Continuity Plan ('BCP') and Disaster Recovery Plans ('DRP') on an ex-ante basis. The BCP/DRP should be prepared in a formal manner, in writing. In case of a security breach and/ or cyber-attack, the CISO should compare the provisions of the CSF, BCP and DRP vis-à-vis the actual impact of a breach/ attack on an ex-post basis.

2.4.5 A crucial aspect of the CSF is human resources. A comprehensive and effective screening process should be implemented in order to prevent possible data breaches and to achieve greater cyber resilience. The CSF should include measures supporting cybersecurity from the commencement till termination of employment of members of staff (and, if and when appropriate, grace period following such termination).

2.4.6 Any employment or engagement contract should contain provisions relating to confidentiality and non-disclosure of information. In the case of contract of employment, the Entity should also ensure that the cybersecurity architecture will not be compromised due to termination or change of employment responsibilities or disciplinary process.

2.4.7 The Entity should conduct a due diligence on relevant individuals and service providers, including *inter alia* software or hardware providers, whose activities or actions could potentially pose a cybersecurity risk.

2.4.8 The Entity should define and enforce restrictions on software installation. Particular consideration should be taken when defining and implementing teleworking and mobile device policy (e.g. remote access policy, Bring Your Own Device (BYOD) policy), which should form part of the written CSF mentioned in Guidance Note 2.4.1 above.

2.4.9 Cybersecurity requirements should also be implemented throughout the software development lifecycle.

2.5 Management of Data and Information

2.5.1 Each Entity should establish and maintain data classification systems, ranging from unrestricted/ public to secret. The labelling of data should define how data is stored and archived with the corresponding access rights and security restrictions in place. Each Entity should further establish and maintain a Data Loss Prevention ('DLP') framework, which puts in place technical and procedural measures to track any movement of confidential data through and out of the organisation in order to detect and flag any unauthorised disclosure of such data.

2.5.2 Each Entity should establish and maintain strict user access control which should be monitored by the CISO. The user access control policy should define physical entry restrictions, including *inter alia* user registration and de-registration, and segregation of types/ levels of access among decision-making bodies, members of staff (including key ICT personnel), independent contractors and service providers. Such user access control should also be extended to digital networks and solutions, such as cloud services, to mitigate the risk attributed to both intentional and unintentional activities of employees who have access to information assets.

2.5.3 Data entry, access controls to program source codes, password-protected formulas and crucial ICT infrastructure should be restricted to privileged users (including the CISO and key ICT personnel). In order to effectively mitigate against critical lock out scenarios, each entity should ensure that its privileged access management policy does not allow for only one privileged user to have administrative access to crucial ICT infrastructures, systems and encryption/ decryption keys. This notwithstanding, passwords should not be shared and each person needs to have unique access credentials.

2.5.4 Each Entity should support a culture of cyber hygiene, including *inter alia*: patch management; password management; policy on idle period; and clear screen policy.

2.5.5 Activity monitoring should be performed on members of staff at all levels, particularly those with greater degrees of access, to minimise the risks of internal sabotage or fraud.

2.5.6 Due diligence and on-going monitoring should be performed on service providers. In order to protect both personal data and trade secret, it is necessary to apply reasonable access restrictions to service providers. Any access rights and restrictions should be clearly defined in the engagement contract as mentioned in Guidance Note 2.4.6.

2.5.7 In the case of internal communication, each Entity should ensure that transmission of data via e-mail or any communicator is conducted in a secure manner, including encryption.

2.5.8 Due to the constant increase in the amount of data being processed, back-up and archiving solutions play a crucial role in terms of an Entity's ability to retrieve sensitive data, when and if necessary. The CISO should ensure that the Entity has a data back-up and archiving policy in place, including the corresponding procedures and secure storage requirements.

2.5.9 In terms of management of data accessible in physical format (or stored on physical devices), attention should be given to management of removable media and physical transfer thereof, including rights and restrictions of access, transmission policy and disposal/ sanitisation procedures thereof. The CISO should also ensure that equipment used in relation to data in physical format undergoes regular maintenance and is subject to access rights and restrictions. Each Entity should also ensure that data in physical format is stored, archived and disposed/ sanitised in a secure manner (including shredding).

2.5.10 One of the key areas which should be established and monitored by the CISO is the emergency evacuation plan. Vulnerabilities which could be exposed during emergency evacuation procedures should be mitigated by prudent policy on protection of critical areas/ facilities/ equipment in case of emergency evacuation and drills.

2.6 Threat Management

2.6.1 The Entity should develop and apply the mentioned proper safeguards to make sure that its systems and networks are fully protected, consequently limiting or containing the impact of a possible cybersecurity breach.

If such a cybersecurity breach occurs, it is vital that this is identified in a timely manner to be able to minimise the potential damage. Thus, the Entity should develop and implement suitable activities for the appropriate identification and minimisation of loss in the occurrence of a cybersecurity event.

2.6.2 Based on the Entity's profile, the CISO should conduct an in-depth threats analysis. Each of the identified threats or factors which could directly and indirectly pose a risk to cybersecurity should be subject to probability-impact analysis as mentioned in Guidance Note 2.3.3.

2.6.3 The CISO should identify, detect and mitigate, when and if necessary, plausible threat agents and factors, which may have considerable effect on the Entity. Traditional risk factors may pose significant risk for the overall business of an Entity, including cybersecurity thereof. In this regard, the CISO should ensure that Threat Management includes, *inter alia*, the following:

i. Natural threats: water damage (flood), fire, weather conditions, Health and Safety threats, etc.;
ii. Insider threats: Clerical errors, identification errors, authorisation errors, sabotage, vandalism, theft;
iii. Privacy threats: unlawful interception, sniffing, data grabbing, unauthorised deep packet inspection, eavesdropping, audio/ video recording;
iv. Environmental threats: power failure, chemical threat, pollution;
v. Macroeconomic threats: financial and liquidity crisis, political crises; and
vi. Other threats: reputational, legal and regulatory threats and implications.

2.6.4 With threat agents becoming more sophisticated, threats related to the existence and operation within the digital space need to be effectively managed. The CISO should establish Information Security Policy ('ISP') covering, *inter alia:*

i. Threat Agents (e.g. script kiddies, hackers, insiders, advanced persistent threat (APT);
ii. Malware, phishing, DDoS attacks;
iii. Hacking of a website/ web application;
iv. Destruction/ modification/ disclosure of data;
v. Mixing test and production data;
vi. Protocol design errors;
vii. Disruption of critical infrastructure of other parties;
viii. Disruption of critical industry-wide services; and
ix. Other: cyber-attacks on the ICT infrastructure (software and/or hardware), insider-threats, social engineering, cyber-attacks on investors, personalised cyber-attacks on the CISO, members of the decision-making body and members of staff of the Entity.

2.6.5 The CISO should ensure that the networks are continuously being monitored by numerous systems, working in real time with intrusion detection measures. Any anomalous or suspicious activity should be immediately investigated further. Those in charge of monitoring and reviewing system reports should be accountable for detection of cybersecurity events and should in turn be well affiliated with the possible impacts of successful cyber threats, in order to be able to formulate the mode of operation required for the response stage.

2.6.6 Through the establishment of an incident response plan, the Entity should apply an organised approach to address and manage the aftermath, with the scope of limiting the damage and reducing recovery time and costs.

It is imperative for any detected cyber threats to be given immediate attention, because it is very difficult to determine their full extent. Any incident must be tackled instantly to prevent it from spreading through the network, neutralising the attack elements and striving to remedy or mitigate the damage that has already been inflicted.

2.6.7 A comprehensive and in-depth inquiry regarding the cyber incident should be performed by analysing the detected event to understand attack targets and methods. This would subsequently enable operative decision making and formulation of possible counter measures to thwart the attack and prevent any similar cyber incidents.

Investigations of cybersecurity incidents should, *inter alia*, assess the following:

i. the origin of the attack;
ii. the attackers' possible scope;
iii. the attack's blast radius;
iv. whether the attack had any significant impact on the system;
v. if the priority given to the situation was reasonable; and
vi. whether the response plan was effectively carried out.

2.6.8 The DRP should incorporate cybersecurity events in order to resume normal operation from disruptions to the systems. Disaster recovery should focus on having procedures in place which are readily available, tested and certified. Lessons learned through simulations or from real-case incidents should be incorporated in recovery plans and processes to enhance their effectiveness.

2.7 Security Awareness and Training

2.7.1 Cybersecurity is bolstered through learning and continuous improvements, and thus the Entity should foster a culture of a learning organisation, with the decision-making body leading by

example. The decision-making body should ensure that adequate financial resources are allocated to awareness sessions for all staff members. The CISO and key ICT personnel should undergo additional specialised training, as necessary.

2.7.2 The awareness sessions mentioned in Guidance Note 2.7.1 should tackle *inter alia* the anticipated effect of the potential cyber threats and data breaches. Staff at all levels should be made familiar with the CSF, BCP and DRP. The CISO should ensure that the awareness sessions focus on internal data classification system, security of data and information (both in transit and at rest), and internal emergency/ incident communication line.

2.8 Compliance and Audit

2.8.1 The decision-making body of each Entity should ensure that internal audit is carried out at regular intervals (unless otherwise indicated by an Entity's risk assessment, at least annually), or following significant changes to the IT infrastructure or operations. Such internal audit shall also include a review of all internal documentation pertaining to cybersecurity (i.e. CSF, BCP, DRP and other policies, standards, procedures, guidelines, etc.). Subsequent to such review, additional clauses/ annexes may be introduced to contractual agreements and contracts of employment, as necessary.

2.8.2 Ad-hoc reviews (based on occurrence of an incident/ attack) should be conducted on an ex-post basis in order to determine the root cause which contributed to the incident/ attack. The relevant procedures or plans should be updated or upgraded accordingly.

2.8.3 Entities are expected to engage, where appropriate with regard to the nature, size and complexity of their business, an independent (external) party to audit their cybersecurity architecture. Unless otherwise indicated by an Entity's risk assessment, such audit should be carried out at least annually. Such audit, must also be carried out upon any material changes/enhancement to the cybersecurity architecture or at such more frequent intervals as may be required by the Authority.

2.8.4 The CISO should comply with applicable legislation/ regulation relating to cybersecurity. Any activity or action taken by members of staff at all levels of the Entity should not be in breach of intellectual property and/ or copy rights.

2.8.5 The CISO is responsible for maintaining all incidents and audit logs which should be made available to the Authority upon request.

2.9 Supplementary Guidance Notes applicable to Issuers of Virtual Financial Assets and VFA Service Providers

2.9.1 General

2.9.1.1. The following Guidance Notes reflect the Authority's approach towards Issuers of Virtual Financial Assets ('Issuers') and VFA Service Providers. The Authority is aware of the challenging task of designing and implementing a robust cybersecurity architecture in view of the sui generis character of Entities operating in the Virtual Financial Assets ('VFA') sector; however, the Authority recommends a risk-based approach in line with the risk profile and proportionate to the size of activity and resources of these operators.

2.9.1.2. The CISO should ensure that any payment transactions are conducted in a secure manner by continuously monitoring and enforcing the use of controls specified in the relevant technical standards and guidelines such as:

i. PCI-DSS;
ii. CCSS;
iii. EBA Guidelines on Internet Payments Security;

iv. EBA Guidelines on Security Measures for Operational and Security Risks under the PSD2; and
v. The Committee on Payments and Market Infrastructures' (CPMI) analytical framework on Distributed Ledger Technology (DLT) in Payment, Clearing and Settlement.

2.9.1.3. Both Issuers and VFA Service Providers are requested to comply with the respective provisions of the respective Rulebooks and follow the Guidance Notes 2.1 to 2.8 above.

2.9.2 Issuers of Virtual Financial Assets

2.9.2.1. The CISO of an Issuer should conduct an advanced ex-ante analysis of the possible threat agents and risk factors affecting cybersecurity of the Entity. In particular, holistic analysis should be undertaken in order to identify possible risks within the Initial VFA Offering period. It is crucial to perform checks vis-à-vis cybersecurity requirements included in the Whitepaper.[1]

2.9.2.2. The CISO of an Issuer should ensure that the Entity's cybersecurity system provides for threat and attack mitigation tools including automatic disconnection from an affected system. Other mitigation tools shall include, *inter alia*: decentralised cybersecurity architecture; kill-switches; safe mode; encryption tools.

2.9.2.3. Given that the Issuers are often start-ups and may opt for cloud based software, it is imperative that the CISO of an Issuer ensures that risks related to solutions such as cloud analytics, business intelligence tools, SaaS applications and APIs are properly mitigated.

2.9.2.4 Based on the analysis of the Issuer's risk profile, the CISO should consider the establishment of multi-factor authentication ('MFA') and at least two-factor authentication ('2FA') for internal and external use. The CISO of an Issuer should also consider the use of secure agents and cybersecurity token providers, who offer, *inter alia*:

i. anti-fraud solutions;
ii. external penetration testing of Issuer's website;
iii. analysis of Smart Contracts for possible errors; and
iv. users' information exchange for detection of threats

2.9.3 VFA Service Providers

The Virtual Financial Assets Regulations (Subsidiary Legislation 590.01 of the Laws of Malta) set out the four (4) licence classes under which subject persons may offer their service in relation to VFAs. This section of the Guidance Notes sets out the specific cybersecurity requirements for each respective licence class.

2.9.3.1. VFAA Class 1

2.9.3.1.1. In line with the provisions set out in the above Guidance Notes, the CISO of a VFAA Class 1 Licence Holder should ensure a suitable cybersecurity architecture to safeguard the respective data held and defend against data breaches.

2.9.3.2. VFAA Class 2

2.9.3.2.1 In addition to the VFAA Class 1 provisions, the CISO of a VFAA Class 2 Licence Holder should ensure adequate mitigation controls to safeguard clients' funds.

[1] As defined in Article 2 of the Virtual Financial Assets Act (Chapter 590 Laws of Malta).

2.9.3.2.2. With regard to wallet creation, the CISO of a VFAA Class 2 Licence Holder should consider the following:

i. Unique address per transaction;
ii. Multiple Keys for signing;
iii. Redundant key for recovery;
iv. Deterministic wallets;
v. Geographic distribution of keys;
vi. Organisational distribution of keys.

2.9.3.2.3. In line with CCSS, the CISO of a VFAA Class 2 Licence Holder should implement tools and policies for secure key generation, including in-house creation of the key, with the creation methodology being validated prior to the use. Cryptographic algorithms and crypto-key configurations should be reviewed for deficiencies and loopholes, through rigorous testing on all cryptographic operations (encryption, decryption, hashing, signing) and key management procedures (generation, distribution, installation, renewal, revocation and expiry). It is also crucial that the keys are tested in line with industry-standard statistical tests for randomness.

2.9.3.3. VFAA Class 3

2.9.3.3.1. VFAA Class 3 Licence Holder should follow the provisions set out in the above VFAA Class 2 Guidance Notes.

2.9.3.4. VFAA Class 4

2.9.3.4.1. In addition to the above Guidance Notes, the CISO of a VFAA Class 4 Licence Holder should ensure rigorous cybersecurity controls in the VFA service provider's operations.

2.9.3.4.2 Given the importance of facilities and policies relating to keys, it is crucial for the CISO to ensure that the back-up key is access-controlled and encrypted. In this respect, specific consideration should also be given to Guidance Note 2.5.3 in order to effectively mitigate against critical lock out scenarios.

2.9.3.4.3. MFA is the preferred method to access keys securely, with 2FA set as a minimum. The authentication should involve combination of an identifier and at least two of the following factors: secure password, MFA token, in-person verification by guard, IP address whitelist, physical key and biometric data.

2.9.3.4.4. The CISO should ensure that the key holders have undergone background checks and that the Entity has means to verify fund destinations and amounts, which should be performed on an ex- ante basis.

2.9.3.4.5. In addition to the provisions of Guidance Notes 2.1 to 2.8, the CISO should ensure that the Entity's CSF include key management procedures and mitigation actions, *inter alia*, a Key Compromise Protocol (which should form part of the Entity's BCP/DRP mentioned in Guidance Note 2.4.4 above), a key retention policy as well as minimum hot and cold storage procedures, and should also provide regular training to key holders.

2.9.3.4.6. The CISO should ensure that Authenticated Communication Channels are used for any form of communication between the VFA Service Provider, key holders and critical/ key operators.

Malta Financial Services Authority

Notabile Road, Attard, BKR3000, Malta
Tel: +356 2144 1155 Fax: +356 2144 1188 Email: communications@mfsa.com.mt
www.mfsa.com.mt