Code of Conduct – Information Security and Acceptable Use

Nordic Aviation Capital

NAC IT/Corporate Legal/ Compliance

Issued: 1 November 2022

Introduction and Purpose

The Information Security and Acceptable Use Code of Conduct is a guide to the requirements and expectations of all NAC Personnel in relation to information security at NAC. Information Security ("IS") is the responsibility of all NAC Personnel and the related policies and procedures lay out the rules and best practices regarding the protection of IS for the business.

This Code of Conduct refers to the Information Security Policy (the "IS Policy") and the Information Security Acceptable Use Policy (the "ISAU Policy" and, together with the IS Policy, the "IT Policies"). NAC IT owns both policies, and it is the responsibility of all NAC Personnel to familiarise themselves and to adhere to those policies accordingly.

NAC Personnel means any person employed by NAC, contractors and any member of the Board while acting for NAC.

Information Security ("IS")

The IS Policy details the responsibilities of all NAC Personnel regarding IS, before, during and after their employment or engagement with NAC. The IS Policy lays out the requirements for the understanding, management, and adherence to important IS matters, including but not limited to the following:

1. Screening requirements prior to employment.
2. Use of assets, systems, and removable media devices.
3. The return of assets and information at the end of employment.
4. Access to network and network services.
5. Approval of access to network and services for other employees and third parties, including the level of access approved, expired access rights, and personal data protection requirements.
6. The use and protection of strong passwords.
7. Encryption of removable devices.
8. Physical protection of systems and information.
9. Documentation of operational procedures for information systems and processing.
10. Protection from malware and IS fraud.
11. Network security and systems management.
12. Software and systems development, testing and implementation.
13. Appropriate IS for vendor screening and access approval.
14. Personal data protection.
15. Incident events – handling, management, and reporting.

For more details on these and other matters please refer to the IS Policy located in the "Policies & Handbooks" section on the Corporate Hub and in the IS Hub.

Information Security Acceptable Use ("Acceptable Use")

The ISAU Policy details the requirements and expectations regarding the acceptable use of IT and acceptable handling of NAC information. It is the responsibility of all NAC Personnel to follow the rules and best practices of Acceptable Use and to familiarise themselves with the requirements of the ISAU Policy. The aim of the ISAU Policy is to protect NAC against virus attacks, network issues, legal issues, and business continuity issues.

There are strict expectations around user behaviour, details of which are laid out in the ISAU Policy, and which include, but are not limited to, the following:

1. Physical security controls at NAC premises.
2. Security of equipment and confidential information outside offices and when travelling.
3. The use and protection of strong passwords.
4. Information classifications - Confidential, Internal, Public and Private.
5. Appropriate use of email and internet - users may **never** download or view sites that are inappropriate, offensive, or illegal.
6. Appropriate private use of email and internet is allowed but should be limited.

For more details on these and other matters please refer to the ISAU Policy located in the "Policies & Handbooks" section on the Corporate Hub and on the IS Hub.

Reporting and Training

The Board (with support from IT) has overall responsibility for ensuring compliance with this Code of Conduct and the Policy by NAC and NAC Personnel. All NAC Personnel has primary and day-to-day responsibility for compliance and familiarising itself with this Code of Conduct and related policies.

NAC's compliance program includes training (both initial and ongoing mandatory annual training), updates and the monitoring of compliance with the Policy. NAC's IT team will also deal with any internal queries and audit internal control systems and procedures to ensure that they are effective.

Reporting will be a crucial part of the Policy's awareness program. If NAC Personnel become aware of, or suspect that, a breach of law or this Code of Conduct or the Policy has occurred, they must promptly report via the appropriate internal channels (including their manager, the next most senior supervisor, or the NAC IT Team), and/ or via the confidential external hotline (contact details for which can be found in the "Policies & Handbooks" section on the Corporate Hub).

NAC Personnel raising concerns in accordance with the Policy will not be subjected to retaliation or penalised in any way for raising a concern. NAC will not tolerate retaliation of individuals who raise matters under this Code of Conduct or the Policy and instances of retaliation will be taken seriously and addressed appropriately.

Please also refer to NAC's Global Whistleblowing Policy concerning reporting generally.

Consequences For Failure to Comply

Failure to comply with applicable laws and regulations are serious offences and strictly prohibited both by law and by the Code of Conduct. NAC Personnel who act in breach of this Code of Conduct or the

related Policies may be subjected to disciplinary measures, up to and including dismissal. They may also risk being prosecuted by the criminal prosecution authorities.

For further information, please refer to NAC's other codes of conduct and compliance policies, available in the "Policies & Handbooks" section on the Corporate Hub.