**SECURITY STANDARDS**

**- FOR THIRD PARTIES ENGAGING WITH INGEUS / APM / CIC**

## General Principles

### 1. Application of these Security Standards

1.1. All references to **"we" or "us"** refer to Ingeus UK Limited, Ingeus Europe Limited, CLNR Horizons Limited t/a CiC, Advanced Personnel Management Group (UK) Limited and their affiliated companies.

1.2. All references to **"you"** refer to any third party:

1.2.1. with whom we share personal data about an identifiable individual,

1.2.2. with whom we share confidential information, and/or

1.2.3. who provide services to us.

1.3. **"You"** also includes your affiliated companies if your affiliates assist you or engage with us in relation to any of the matters in 1.2.1 to 1.2.3 above.

### 2. General Obligations

2.1. You must have appropriate management policies and processes in place to govern your approach to the security of your networks and information systems.

2.2. You must take appropriate steps to identify, assess and understand security risks relating to your network and information systems which support the operation of essential functions within your organisation. This includes having an overall organisational approach to risk management.

2.3. You must determine and understand everything required to deliver, maintain or support the networks and information systems which are necessary for the operation of any contract between you and us. This includes data, people and systems, as well as any supporting infrastructure.

2.4. You must understand and manage security risks to networks and information systems which support the operation of essential functions within your organisation that arise because of dependencies on external suppliers. This includes ensuring that appropriate measures are taken where third party services are used.

2.5. You must define, implement, communicate and enforce appropriate policies and processes that direct your overall approach to securing systems and data that support your operations.

2.6. You must understand, document and manage access to networks and information systems supporting the operation of essential functions within your organisation. Users (or automated functions) that can access data or services must be appropriately verified, authenticated, and authorised.

2.7. You must protect data (both in digital and in hardcopy, whether being stored or transmitted) from actions such as unauthorised access, modification, or deletion that may cause an adverse impact on operational delivery.

2.8. You must protect from cyber-attack all network and information systems and technology that are critical for your operations.

2.9. You must build appropriate resilience against cyber-attack into the design, implementation, operation and management of systems that support your operations.

2.10. You must train and equip staff to protect the security of network and information systems while carrying out their roles.

2.11. You must monitor the security status of the networks and systems supporting essential functions in your organisation in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.

2.12. You must detect, within networks and information systems, malicious activity affecting, or with the potential to affect business operations.

2.13. You must have a well-defined and tested incident management process and must report all incidents affecting us to us as soon as they arise.

2.14. You must understand the root causes of security incidents and take appropriate remedial action as part of your incident management process.

**Specific Obligations**

Within your organisation, you must:

3. **Governance**

3.1. Ensure that responsibilities for compliance with laws and regulations are assigned and understood.

3.2. Implement governance practices which establish, resource, and maintain information security practices.

3.3. Publish and maintain policies and communicate information security standards to all your employees, contractors and officers (collectively your **"staff').**

3.4. Identify any legal or regulatory requirements which may impact your approach to information security.

3.5. Review laws and regulations for changes which impact compliance at least once a year.

3.6. Where you make changes to the Suppliers' Applications which could have an impact on our ability to meet compliance requirements, you must, where reasonably required by us, work with our global and local information security teams to implement controls that meet our compliance requirements.

4.

**Risk Management**

4.1. Review information security risks using your risk management and governance framework and localised information security forums.

4.2. Undertake and regularly review information security risk assessments.

4.3. Undertake information security assessments and privacy impact assessments when you make changes to your business or when there are legal / regulatory changes and review these at least once a year.

4.4. Where reasonably required by us, work with our global information security team and our local privacy team to implement security measures to manage identified information security risks in your systems and organisation. Mitigate identified

information security risks in your systems and organisation.

5. **Asset management**

5.1. Identify, document and maintain an inventory of assets used by your organisation to store or otherwise process information (collectively **"assets").** Specifically:

5.1.1. This obligation extends to all operating systems and firmware on your hardware, such as servers, end user computers and network devices. You must keep track of your operating systems and promptly decommission them when they reach their end of life **(EOL).**

5.1.2. You must only use software which is supported by a supplier who provides regular security updates. You must remove unsupported software from your devices.

5.1.3. Your software must be licensed. You may use free and open source software as long as you comply with any licensing requirements.

5.1.4. Where possible, you must enable auto updates, and:

5.1.4.1. You must follow a documented process where auto updates are not available or are not applied.

5.1.4.2. Where updates are not automatically applied, you must update your operating systems, firmware and applications with vulnerabilities scoring CVSS 7.0 or more within 14 days of release.

5.1.5. You must remove older software from your devices as soon as the manufacturer stops supporting it.

5.1.6. You must install firewalls between your corporate network and the Internet.

5.1.7. You should have firewalls for home-based staff. If home-based staff do not use a corporate virtual private network **(VPN)** to connect to your corporate network, you must ensure that they use the software firewall of their device's operating system.

5.1.8. You must change the default password on all routers and firewalls, including those that come with a pre-configured unique password.

5.1.9. Your Firewalls will limit the use of internet services from your internal network using destination IP address and port OR URL filters. Where new access requests are required, a formal change will be approved via the change management process.

5.2. Allocate ownership of all assets in your inventory to an asset owner.

5.3. Classify all assets in your inventory with reference to the legal requirements applicable to them, their value, their criticality and sensitivity to unauthorised disclosure or modification.

5.4. Identify, document and implement rules for the acceptable use of information and assets.

5.5. Ensure that your staff return your assets when their contract with you terminates.

5.6. Develop, implement and maintain an appropriate set of procedures to label information consistent with your organisation's information classification scheme.

5.7. Develop, implement and maintain procedures for handling assets consistent with your organisation's information classification scheme.

5.8. Develop, implement and maintain procedures for managing removable media consistent with your organisation's information classification scheme.

5.9. Ensure that media containing information is securely disposed when it is no longer required.

5.10. Protect media containing information against unauthorised access, misuse or corruption during transportation.

6. **People Management**

6.1. Perform background verification checks on all candidates for employment in accordance with relevant laws and regulations. Where warranted by the nature of your business or if we require this, you should also perform background checks on your contractors and officers. All checks must be proportional to your business requirements, the classification of the information to be accessed and the perceived risks of granting access.

6.2. Require your staff to comply with your organisation's information security requirements, policies and procedures, in their contracts with your organisation.

6.3. Provide awareness training and provide regular updates about information security requirements, policies and procedures to all your employees and, where relevant, your contractors and officers, as relevant for their function.

6.4. Implement, communicate and maintain a formal process which allows you to take action against staff who breach your information security requirements, policies and procedures.

6.5. Make it clear to your staff which of your information security requirements, policies and procedures will continue to apply after their contract with you has terminated or changed.

7. **Access Controls**

7.1. Establish, document and regularly review an access control policy consistent with your information security requirements.

7.2. Only grant access to your network and network services to users who are specifically authorised to use them.

7.3. Implement a formal user registration and de-registration process to enable assignment of access rights.

7.4. Implement a formal user access process which allows access rights for all user types to all systems and services to be assigned or revoked.

7.5. Restrict and control the allocation and use of privileged access rights to users.

7.6. Implement a formal management process to allocate and control secret authentication information.

7.7. Ensure that asset owners regularly review users' access rights.

7.8. Remove the access rights of staff and external guest users to information and to your assets when their contract with you terminates or adjust their access rights if their contract with you changes.

7.9. Require users to follow your organisation's requirements, policies and procedures when using secret authentication information.

7.10. Restrict access to information and application system functions consistent with your access control policy.

7.11. Where required by your access control policy, control access to systems via a secure log-on procedure. Specifically:

7.11.1. You must ensure that user accounts (such as logins to laptops and accounts on servers) are only provided after they have been approved by a person with a leadership role in the business.

7.11.2. You must ensure that no devices can be accessed without entering a username and password.

7.11.3. You must ensure that users do not share accounts.

7.11.4. You must terminate user access to your systems when their agreement with your organisation terminates.

7.11.5. When a staff member's role changes, you must change their previous access permissions and give them access only to those files, folders and applications that they need to perform their new role.

7.11.6. You must have a formal, written process for granting access to systems at administrator level. This process should include approval by a person with a leadership role in the business .

7.11.7. Administrative privileges must be managed to ensure they are only used when necessary and do not expose systems to unnecessary risk. Access for administrative tasks should be restricted and controlled to prevent misuse or prolonged elevated privileges. Measures must be in place to separate routine user activities from administrative functions and to safeguard cloud service administration through appropriate account management practices.

7.11.8. You must track all people who have been granted administrator accounts, by means of a list or formal record.

7.11.9. You must regularly review the list of people who have administrator access. Depending on your business, this might be monthly, quarterly or annually. You must remove administrator accounts from all users who no longer need administrative access to carry out their role.

7.11.10. You must ensure that people who have access to your organisational data and services choose strong and unique passwords and that they update their passwords regularly.

7.11.11. You must implement, communicate and maintain a process that requires staff to change passwords quickly if you know or suspect that a password or account has been compromised.

7.11.12. You must enable multi-factor authentication **(MFA)** for users and administrators (for example a text message, a one time access code or notification from an authentication app) where your systems and cloud services support this.

7.12. Implement interactive password management systems that only allow users to use difficult-to-guess passwords.

7.13. Restrict and tightly control the use of utility programs that can override your system and application controls.

7.14. Restrict access to all program source code used within your organisation.

8. **Cryptography**

8.1. Develop, implement and maintain a policy for using cryptographic controls to protect information.

8.2. Develop, implement and maintain a policy for using and protecting cryptographic keys during their lifecycle.

9. **Physical Security**

9.1. Define and use security perimeters to protect areas that contain sensitive or critical information and information processing facilities.

9.2. Protect secure areas by appropriate entry controls to ensure that only authorised staff can gain entry.

9.3. Design and apply physical security for offices, rooms and facilities.

9.4. Design and apply physical protection against natural disasters, malicious attacks or accidents.

9.5. Design and apply procedures for working in secure areas.

9.6. Ensure that access points (such as delivery and loading areas) and other points where unauthorised persons could enter the premises are controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.

9.7. Protect equipment from environmental threats, hazards and unauthorised access.

9.8. Protect equipment from power failures and other disruptions caused by failures in supporting utilities.

9.9. Protect power and telecommunications cabling carrying data and/or supporting information services from interception, interference or damage.

9.10. Maintain equipment to ensure its continued availability and integrity.

9.11. Ensure that equipment, information or software is not taken off-site without prior authorisation from the owner, licensor, lessor or equipment supplier (as applicable).

9.12. Ensure that off-site assets are sufficiently secured, taking into account the risks of working outside your organisation's premises.

9.13. Verify all equipment containing storage media to ensure that any sensitive data and licensed software have been removed or securely overwritten prior to disposal or re-use.

9.14. Ensure that users protect unattended equipment.

9.15. Implement and enforce a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities.

10. **Security Operations**

10.1. Document and communicate information security operating procedures to all users who need them.

10.2. Implement and enforce change control processes for changes to your organisational processes, business processes, information processing facilities and systems where these affect information security.

10.3. Monitor your organisation's use of resources, including projections of future capacity requirements, to ensure that the system continues to perform to the required standard.

10.4. Identify users who are foreign nationals where government agencies require this, including seconded foreign nationals, and keep a record of their specific nationality.

10.5. Implement and communicate malware detection, prevention and recovery controls to users. Specifically, you must:

10.5.1. ensure that your systems prevents access to known malicious websites,

10.5.2. prevent all users from installing unauthorised applications on your organisation's devices,

10.5.3. maintain an up-to-date list of approved applications and ensure that users only install these applications on their devices (including staff-owned devices). You may use mobile device management **(MDM)** software to do this, except if you can meet this requirement using good policy, processes and training of staff.

10.6. Make backup copies of information, software and take system images regularly and test these regularly in accordance with your organisation's backup policy (or any contractually agreed backup policy).

10.7. Produce, maintain and regularly review event logs recording user activities, exceptions, faults and information security events.

10.8. Protect your organisation's logging facilities and log information against tampering and unauthorised access.

10.9. Ensure that system administrator and system operator activities are logged and that the the logs are protected and regularly reviewed.

10.10. Ensure that the clocks of all relevant information processing systems within your organisation or security domain are synchronised to a single reference time source.

10.11. Implement procedures to control the installation of software on operational systems.

10.12. Obtain information about technical vulnerabilities of your information systems in a timely fashion, evaluate your organisation's exposure to these vulnerabilities and take timely and appropriate measures to address the associated risk.

10.13. Implement rules governing the installation of software by users.

10.14. Plan audit requirements and activities involving verification of operational systems so as to minimise disruptions to your business processes.

10.15. Manage and control networks to protect information in your systems and applications.

10.16. Identify security mechanisms, service levels and management requirements applicable to all your network services and include these in network services agreements where possible, whether these services are provided in-house or outsourced.

10.17. Segregate groups of information services, users and information systems on your systems and networks.

10.18. Protect business information transferred via electronic messaging platforms.

10.19. Implement and maintain formal transfer policies, procedures and controls to protect the transfer of business information through all types of communication platforms.

10.20. Ensure that business information is securely transferred between the organisation and external parties.

10.21. Ensure that confidentiality agreements are executed where there is a need to protect business information, and that you regularly review the categories of information requiring contractual protection against disclosure.

11. **Systems Acquisitions and Development**

11.1. Ensure that all new information systems and/or enhancements to existing information systems comply with your security requirements.

11.2. Protect business information in application services passing over public networks from fraudulent activity, contractual disputes and unauthorised disclosure and/or modification.

11.3. Protect business information in application services against incomplete transmission, mis-routing, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

11.4. Establish rules for and apply those rules to the development of software and systems.

11.5. Control changes to systems during their development lifecycle via formal change control procedures.

11.6. Review and test business critical applications when changing operating platforms, to ensure there is no adverse impact on your operations or security.

11.7. Discourage unnecessary modifications and strictly control all changes to off the shelf software packages.

11.8. Document, implement and maintain principles for engineering secure systems that must be applied to all information systems that your organisation uses.

11.9. Assess the risks associated with individual system development and integration efforts during the entire system development lifecycle.

11.10. Establish and protect secure development environments for system development and integration efforts during the entire system development lifecycle.

11.11. Supervise and monitor outsourced system development.

11.12. Test security functionality during development.

11.13. Carefully select, protect and control test data.

12. **Supplier Relationships**

12.1. Assess and report on the information security controls of third parties to us when requested.

12.2. Evaluate and audit the compliance of third parties with relevant security standards, including the third party's ability to secure the information entrusted to them.

12.3. Agree and document your information security requirements and processes for mitigating the risks caused by giving third parties access to your organisation's assets.

12.4. Agree, establish and document the information security requirements with each third party who accesses, processes, stores, communicates or provides IT infrastructure components for your organisation's information.

12.5. Contractually oblige your suppliers to address the information security risks associated with information and communications technology services and their product supply chain.

12.6. Regularly monitor, review and audit supplier service delivery.

12.7. Manage changes to services provided by third party suppliers, including by maintaining and improving existing information security policies, procedures and controls, taking account of the criticality of business information, systems and processes involved and re-assessing the risks.

13. **Incident Management**

13.1. Report information security events via the appropriate process and management channels as quickly as possible.

13.2. Oblige your staff to note and report any actual or suspected information security weaknesses in your organisation's systems or services.

13.3. Assess all information security events and classify those that are information security incidents.

13.4. Respond to information security incidents in accordance with your documented procedures.

13.5. Proactively use knowledge gained from analysing and resolving information security incidents to reduce the likelihood and impact of future incidents.

13.6. Define and apply procedures to identify, collect, acquire and preserve information which can serve as evidence.

13.7. Gather and maintain evidence that your organisation has implemented security measures in accordance with your security requirements and any contractual requirements agreed to between you and us.

13.8. Conduct both internal and obtain independent external assessments and tests of security controls and undertake remediation activities where those controls are unsatisfactory in an agreed schedule with us.

14. **Business Continuity and Disaster Recovery**

14.1. Determine your organisation's requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

14.2. Establish, document, implement and maintain processes and controls that maintain the required level of information security during an adverse situation.

14.3. Regularly review existing information security continuity controls to ensure that they will continue to be effective during an adverse situation.

14.4. Build sufficient redundancy into your organisation's information processing facilities to meet availability requirements.

15. **Compliance**

15.1. Identify, document keep updated all relevant legislative statutory, regulatory and contractual requirements and how your organisation meets these requirements - for each information system and for your organisation as a whole.

15.2. Implement appropriate measures and procedures to ensure compliance with legislative, regulatory and contractual requirements relating to intellectual property rights and your organisation's use of proprietary software products.

15.3. Protect records against loss, destruction, falsification, unauthorised access and unauthorised release, in accordance with legislative, regulatory, contractual and business requirements.

15.4. Ensure that and protect the privacy of personally identifiable information as required in relevant legislation and regulation.

15.5. Use cryptographic controls in compliance with all relevant agreements, legislation and regulations.

**16. Artificial intelligence**

16.1. The supplier must not introduce any Artificial Intelligence into the product or service without prior written consent and approval from Ingeus/APM Cyber Security Team