A: TECHNICAL MEASURES

1. Access Controls and Authentication: access to systems by users, including employees, is secured by a username and unique password defined and updated according to relevant standards. Authentication measures are implemented and the concept of minimum permissions needed for relevant context or role based on minimum access or principals.

2. Network Security: one or more firewalls or equivalent protections are used to protect data and control traffic and connections into and out of technology resources, such as storage and compute resources.

3. Malware Protection & Intrusion Detection: equipment and servers are protected with appropriate real-time anti-virus, anti-spyware and anti- malware software. Intrusion protection and prevention systems are implemented.

4. Device Security: devices, including laptops and mobile phones are configured in a secure manner, including implementation of device level encryption where possible to protect data stored or cached locally on the device.

5. Encryption of Data in Transit: where data transfer is permitted robust encryption solutions such as TLS 1.2 are used to ensure the security of data in transit.

6. Encryption of Data at Rest: in addition to device encryption measures utilised for suitable context additional arrangements are used according to the context and technical architecture. Arrangements such as AES-256 with KMS key management are used to ensure the security of data at rest.

7. Backups and Recovery: regular backups are conducted to ensure that data is stored safely and securely and remains accessible, even, for example during temporary outage impacting primary hosting resource.

8. Updates and Patching: regular software updates are implemented using patch management software and/or other technical solutions to keep latest

9. Secure Deletion: timely deletion is applied to systems and resources used for data storage or processing through measures which are suitable and effective for each relevant system or storage medium. For example in an active system data no longer needed may be deleted or over-written, shredding may be used for paper or similar physical files and magnetic or other effective destruction technique may be used for electronic storage media upon retirement or de-commissioning in line with relevant policies and procedures.

10. Logging and Monitoring: systems are subject to regular monitoring, oversight, review and controls to ensure data is secure and uncompromised. System logging is used where suitable and systems are hardened and improved where possible based on ongoing improvement and review process.

B: ORGANISATIONAL / OPERATIONAL MEASURES

11. Security Governance: industry standards are referenced as part of applicable governance arrangements with mapping against applicable technical standards.

12. Policies and Procedures: policies and procedures relating to the physical security of data on premises, the secure storage, deletion and disposal of confidential information, the use of personal devices for work purposes, and the prohibition of use of personal email for work purposes and other relevant topics are documented and mandated.

13. Training and Awareness: employees receive mandatory information security training. The importance of the role of each individual in protecting data is emphasised and emergent risk scenarios are referenced to ensure training remains up to date.

14. Risk Management: Risks are assessed and managed following established methodology. Reviews, and where applicable audits, ensure threats are identified, scored, and treated with appropriate controls.

15. Incident Management: A formal incident response process defines escalation paths and responsibilities. Incidents are logged, investigated, and used to strengthen preventive controls.

16. Business Continuity: Business continuity and disaster recovery plans are maintained and tested. The backup strategy ensures services remain available even during disruption.