## ANNEX II TECHNICAL AND OPERATIONAL MEASURES (TOMs) TO PROTECT PERSONAL DATA

When processing Personal Data on behalf of Client – Arcadis shall provide an appropriate level of security to protect the Personal Data in accordance with Clause 4. of the DPA. Arcadis shall for a minimum implement the following security measures:

### *1. Information security management system*

Arcadis' information security management system will be aligned with international standard ISO27001, in order to: protect the confidentiality, availability, and integrity of the Personal Data, including policies, procedures, guidelines, processes and technical solutions; protect Personal Data from misuse or accidental, unlawful or unauthorized destruction, loss, alteration, disclosure, acquisition or access; establish the basic principles and rules of Information Security within Arcadis' organisation. The information security management system is periodically reviewed following the evolution in Arcadis' information risk landscape.

### *2. Information Classification and Access Control*

Arcadis acknowledges that information must be protected against loss and infringements on integrity and confidentiality. Each department or other organizational unit of Arcadis is required by policy to assess risks to information assets and periodically check the level of security through security reviews.
Information is classified into the appropriate number of categories in accordance with industry standards, and for each classification the appropriate levels of security controls have been implemented.
All employees of Arcadis are assigned unique User-IDs. Only authorized individuals can grant, modify, or revoke access to an information system that uses or houses Personal Data, and access may be granted for valid business purposes only.
User administration procedures define user roles and their privileges, how access is granted, changed and terminated; address appropriate segregation of duties; and define the logging/monitoring requirements and mechanisms. Arcadis maintains appropriate physical and electronic security measures to create and protect passwords.

### *3. Virus and Malware Controls*

Arcadis installs and maintains anti-virus and malware protection software on the system. Arcadis ensures appropriate logging and monitoring to enable recording of IT security-related actions.

### *4. Physical Security*

Arcadis maintains adequate security systems at all Arcadis sites at which an information system that uses or houses Personal Data is located. Secured areas employ various physical security safeguards, including use of security badges (identity-controlled access) and security guards stationed at entry and exit points. Visitors may only be provided access where authorized.

### *5. Organizational aspects concerning information security*

Roles and responsibilities around information security have been established, including a role appointed responsible of cyber security and IT compliance department. Three lines of defence have been implemented in order to assess and monitor the effectiveness of the implemented IT and security controls.

### *6. System Integrity and Availability*

Arcadis maintains network security using adequate equipment and industry standard techniques, including firewalls, intrusion detection and/or prevention systems, access control lists and routing protocols.
In the event of degradation or failure of the information infrastructure, Arcadis implements appropriate disaster recovery and business resumption plans. Back-up copies of critical business information and software are created regularly and tested to ensure recovery. Contingency procedures are tested at least annually.

### *7. Security Incidents*

All Arcadis personnel are required to report any observed or suspected Privacy Incident in accordance with appropriate incident response procedures.

### *8. Training & Compliance*

Arcadis personnel are required to read, sign, and abide by the Arcadis information security management system and its policies, procedures and guidelines as a condition of employment. Personnel are subject to disciplinary measures for violations of these policies. New employees of a certain job level undergo reference checks, also education verification and criminal background checks are undertaken where required.
In addition, Arcadis implements a security awareness program to train personnel about their security and privacy obligations. This program includes training about data privacy and security practices; physical security controls; and security incident reporting
Arcadis regularly monitors the implemented security measures and implementation of new security requirements. Compliance with Arcadis' information security policies is accomplished through annual training, periodic reviews of local and organization-wide policies and procedures, and audit.