1 Appendix L – DCC's Standard Requirements regarding System and Data Security

1.1 Data and System Security

Integrity, Availability and Confidentiality of Data is a critical requirement for Dublin City council's Information Systems. It is a requirement that the processing and storing of all Data, is restricted to the European Economic Area. The system must ensure security and privacy by design. The system and relevant Data must comply with privacy and data protection requirements of the GDPR.

1.2 Independent System Assessment

It is Dublin City Council's policy that proposed systems will be independently assessed with regard to security including vulnerability scanning and penetration testing by Dublin City Council or by an independent service provider. The system vendor will be required to address all security issues identified by such review.

In the case of prior penetration testing and/or vulnerability scanning performed on the application. Proof of the same would be required along with documentation justifying the actions taken towards securing the application against the highlighted issues.

Periodic security assessments of the system to be conducted by Dublin City Council or by an independent service provider. It would be expected of the successful Tenderer to resolve the identified security issues on a predetermined timeline based on the criticality of the issue discovered.

Dublin City Council will not incur any extra cost for the vendor making these changes and the system will not be considered acceptable until such issues are addressed in an acceptable manner and timeframe.

1.3 Multifactor Authentication

It is mandatory that systems support multi-factor authentication (MFA) to ensure the security and authenticity of the accounts involved. MFA should be in place for both user and admin accounts,

In the event that MFA is not currently supported, the successful tenderer must commit to make MFA available during the development/configuration stage.

1.4 Security Controls

Hosting shall be provided either in a commercial data centre, infrastructure as a service cloud provider or from the vendors' data centre. This must be fully described including all services contracted from any third party.

As minimum requirements, the following elements must be considered:

a) Hosting Controls

Policies, procedures, supporting business processes and technical measures to prevent the execution of malware on the proposed technical infrastructure must be in place.

Technical measures for the timely detection of vulnerabilities and appropriate remediation process must be in place.

Security mechanisms to protect the data centre perimeter and prevent data leakage must be in place.

Vendors must have well established processes and procedures in relation to intrusion detection and incident response mechanisms.

i. Environment Segregation

Security controls regarding segregation if the environment is shared by multiple tenants must be in place.

Environment segregation with regard to separation of development, testing and operational environments must be facilitated and aligned with ISO 27001, NIST or similar framework.

ii. Identity Management

User access policies, procedures and technical measures must be implemented, for ensuring appropriate identity, entitlement, and access management to data and corresponding system components.

These policies and procedures must cover (but not limited to):

- Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or another customer (tenant))
- Account credential lifecycle management from instantiation through revocation
- Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor).

iii. Business Continuity and Disaster Recovery

Vendors must have well established processes for business continuity planning and provide information and evidence on how often business continuity plans are tested.

Vendors must provide information and evidence on the following points concerning Disaster Recovery.

- Individuals responsible for performing the recovery task.

- A timeline for recovery.
- The defined process to implement data recovery.
- Vulnerability management

All operating systems and application components must be kept at N-1 release at all times.

Where emergency security patches need to be applied, the vendor must commit to apply these patches within 24hrs. Vendors must also provide Information on the ongoing vulnerability management process

b) Certificates

It is a requirement that the proposed data centre hosting the application is ISO27001 (or similar certification) and Tier1 or Tier2 accredited.

c) Application Security

Applications and interfaces (APIs) shall be designed, developed, and deployed following industry acceptable standards (e.g., OWASP for web applications or similar) and adhere to applicable legal, statutory, or regulatory compliance obligations.

Vendors must provide executive summary/reports and evidence of previous penetration testing assessments conducted on the systems and highlight the improvements made concerning security based on the assessments.

END OF DOCUMENT