City of Dublin Education and Training Board

Outsourcing and Acquisitions policy

Document version	2
Drafted by	ETBI (ICT Group)
Responsibility for this policy in City of Dublin ETB	Director OSD and Head of IT
Reviewed by Senior Leadership Team (SLT)	12 October 2021
Approved by Chief Executive	12 October 2021
Noted by Board	21 October 2021
To be reviewed	1 year from date of approval by CE

Contents

1 Introduction

1.1 Purpose of this Document

The purpose of this policy is to protect any City of Dublin ETB Corporate Data including Sensitive Data to which third-party access is given. It requires that third-party services meet the outlined security and quality standards.

In addition, it requires assignment of roles and responsibilities for monitoring third-party services, managing relationships, and managing contracts.

Compliance with this policy forms part of City of Dublin ETB governance requirements, including compliance with the Data Protection Act 2018, the General Data Protection Regulations, the Children First Act 2015 and general industry standard best practice.

1.2 Scope

This policy applies to all External Users who provide services to City of Dublin ETB. This policy is effective as of the issue date and does not expire unless superseded by another policy.

1.3 Policy Review, Approval and Continuous Improvement

In line with best practice, this policy has been approved by senior management, along with its commitment to continually improve the protection of all City of Dublin ETB Corporate Data including Sensitive Data and the protection of personal data where City of Dublin ETB is a controller or processor. This document will be reviewed annually by senior management, to ensure alignment to appropriate risk management requirements and best practice for the management procurement and third party engagements.

1.4 Definitions

A full range of definitions is available in the ICT Frameworks Policy.

2 Outsourcing and Acquisitions Policy

All third-party vendors (includes business partners) or service providers must comply with the City of Dublin ETB policies and security requirements.

1) The third-party should have its own defined security policies, which should be supported by documented procedures, and in line with City of Dublin ETB security policies. These should be made available to the ETB on request.

2) All outsourcing or exchange of information must be compliant with GDPR guidelines and the Data Processing Policy.

3) Any variations to the third-party's compliance with the City of Dublin ETB ICT Framework policies and standards must be recorded in writing and must be signed by both parties.

4) City of Dublin ETB must have the right, throughout the term of its agreement with the third-party, to undertake security reviews, which could be in the form of a penetration test, at an agreed and convenient time, to ensure that data has the appropriate level of security protection. If physical security assessments are warranted, an unscheduled physical security assessment may be required without prior notification to the third-party.

5) All contractual agreements with the third-party must have a specific written clause stating that City of Dublin ETB has the right to audit any service delivered on its behalf, with prior notification. All findings and recommendations must be documented and presented to the third-party service provider and City of Dublin ETB senior management for implementation within an agreed time period.

6) The third-party must nominate a central point of contact for security-related activities to undertake the following:
    1. Assignment of supplier security resources;
    2. Interfacing with City of Dublin ETB on security requirements;
    3. Implementation of security requirements in accordance with these Policies;
    4. Provide monthly security reports if applicable;
    5. Coordinate the requirements of this policy with subcontractors where such an arrangement has been agreed with City of Dublin ETB;
    6. Make available systems and personnel to enable City of Dublin ETB to perform internal and external audits within the parameters agreed between City of Dublin ETB and Supplier, and supply the security Services and keep and disclose the documentation agreed to be supplied to support City of Dublin ETB audits;
    7. Assisting with the completion of Data Protection Impact Assessments (DPIAs)where requested;
    8. Agreeing the requirements and recommendations of Data Processing Agreements (DPAs) and Data Protection Impact Assessments (DPIAs).

7) Where there is a need to pass or provide access to City of Dublin ETB information classified as Internal-Use-Only or higher to a non-City of Dublin ETB person or company, then a Non-Disclosure Agreement (NDA) must be completed **prior** to the exchange of any information.

    At the end of such arrangements, City of Dublin ETB Corporate Data, information and

media must be recovered where relevant. This applies to third parties and subcontractors, where the third-party may outsource the information.

8) All RFI/RFP/RFT documents (Requests for Information/Proposal/Tender), must refer to City of Dublin ETB ICT Framework Policy to ensure that they are built into the specification and included in any cost estimates. As a pre-requisite, compliance with City of Dublin ETB security criteria and standards **[should be, is]** required.

9) Where remote administration/maintenance is provided, the third-party must confirm that there is no direct or indirect customer network coupling via its management/ administration network infrastructure.

10) Where permitted, remote access for supplier maintenance or diagnostics purposes into City of Dublin ETB should be strictly controlled so as to protect the security of the system. This must have prior authorisation by the IT Department in City of Dublin ETB and should be strictly limited to the time necessary to perform the required service. All remote access to City of Dublin ETB systems must follow an approved remote access method and be in compliance with the Remote Access Security Policy.

11) Any suspicious activity must be promptly reported to City of Dublin ETB's IT Department

12) City of Dublin ETB should maintain a list of all ICT services that are outsourced, including authorisation to outsource from the relevant line manager.

A signed contract and/or SLA must be in place between City of Dublin ETB and the third party. The following ICT criteria are best practice and may be included in a contract for service or an SLA where appropriate:

a. A signed contract and/or SLA must be in place;
b. A statement of compliance with the security policies contained in this document;
c. The contract has to include a right for the ETB to audit, or have audited, the third-party, which can include compliance monitoring in certain circumstances;
d. The contract has to include a suitable Non-Disclosure Agreement (NDA)
e. Security responsibilities must be clearly defined;
f. Notification procedure and security incident management;
g. In case a network connection to or from the third-party (or any subcontractor); the connection has to comply with City of Dublin ETB remote access policies;
h. Where dealings may result in software or data being transferred onto City of Dublin ETB systems, the contract must include the requirement for the supplier to scan all such software and data using the latest available virus protection software **prior** to it being transferred to City of Dublin ETB;
i. Return or destruction of the information on completion of the agreement;
j. Change management procedure;
k. Service level and acceptable parameter indicators;
l. Follow-up reports of service level, as well as penalisation in the case of noncompliance with the agreed parameters;
m. Access control policy for information and the systems which process such information;
n. Data Processing Agreements (DPA) to ensure due diligence and privacy of personal data must be agreed to whereby roles and responsibilities for data controllers, data processors and sub-processors are established;
o. Any recommendations arising from risks identified in the course of a Data Protection Impact

Assessment (DPIA);

p. Where remote administration/maintenance is provided, the third-party has to ensure that there is no direct or indirect customer network coupling via their management/administration network infrastructure.

When the development of a bespoke system is outsourced to a third-party, the following points must be in the written contract, in addition to those specified in point above:

a. The ownership, intellectual property rights and licensing agreements of the developed software should be clearly defined;
b. Application security requirements should be clearly defined;
c. Compliance with the applicable security requirements should be defined and monitored;
d. The quality and security of the delivered software should be guaranteed by contract, making the third-party responsible for any damages incurred by the company due to shortcomings in the software;
e. The third parties will sign confidentiality and non-disclosure agreements and data processing agreement where appropriate;
f. Where the system is being provided via third or fourth party hosting, full disaster recovery procedures need to be detailed.

3 Enforcement

Individuals found to be in breach of this Outsourcing and Acquisitions Policy, may be subject to disciplinary action, up to and including contract termination or dismissal where appropriate. Should an investigation regarding compliance with this policy determine that there is a case to answer by a User / responsible third party, the matter will be referred into the appropriate stage of the relevant procedure as appropriate to that User / responsible third-party.