Secure Development of Cloud Services Policy

Reference: CLD DOC 14.2.1
DocumentKits Issue No: 1.0
Organisation Issue No:
DocumentKits Issue Date: 09/06/2020
Organisation Issue Date:

1. Scope

Organisation Name's development environment, staff, process and infrastructure are covered by this policy.

2. Responsibilities

The Chief Information Security Officer (CISO) is responsible for securing the development environment against threats.

The Project Manager is responsible for the security of any given Cloud development project, and for ensuring that privacy requirements are accounted for during the development process.

<<Content removed for sample purposes>>

3. Procedure

"Describe Organisation Name's approach to ensuring the security of development for Cloud services. This should align with the same core principles as your primary secure development policy, and include policy statements covering Cloud service considerations specifically, including:

- Virtualisation security;
- How you will monitor and ensure sufficient capacity for the service throughout its lifecycle;
- Use of customer or third-party programs within the operational Cloud environment, and any necessary security and privacy measures;
- Any unavoidable use of personally identifiable information (PII) for testing purposes and how security and privacy are assured to be equivalent to production environment protection for PII;
- The need to minimise processing of PII by default;
- <<Content removed for sample purposes>>
- <<Content removed for sample purposes>>
- <<Content removed for sample purposes>>
- How secure disposal and reuse of resources, including customer data (whether at termination or otherwise), are ensured in line with the Return of Customer Assets Procedure, how this information is communicated to customers, and how it will be ensured that such information is included in service agreements;
- <<Content removed for sample purposes>>
- <<Content removed for sample purposes>>

- <<Content removed for sample purposes>>
- Requirements for network segregation and tenant isolation, including segregation between tenants in multi-tenant environments, segregation between the internal administration environment and the Cloud service customer's Cloud computing environment, and the risks associated with customer use of third-party programs;
- Access to customer data, including PII, by Organisation Name's employees;
- <<Content removed for sample purposes>>
- <<Content removed for sample purposes>>
- <<Content removed for sample purposes>>
- Access controls and authentication techniques for Organisation Name's employees and for customers, including for administrative users and users with other kinds of privileged access, and specifications for the use of such functions;
- Management procedures for allocation of secret authentication information and how these will be communicated to customers in a secure manner;
- <<Content removed for sample purposes>>
- Inclusion and application of cryptographic controls as indicated by risk assessment, and methods for communicating information on the use of cryptographic controls to customers, without compromising the security or effectiveness of those controls;
- Methods to communicate with customers of the services in respect of general use, change management and other required communications;
- <<Content removed for sample purposes>>
- <<Content removed for sample purposes>>
- <<Content removed for sample purposes>>

You should link each of these to a procedure (including Secure Development Procedures) describing the specific requirements. Several of these topics are further described in ISO 27017.

You will need to create documentation covering the following items that can be made available to customers on request:

- The scope of information security incidents that the Cloud service provider will report to the Cloud service customer.
- The level of disclosure of the detection of information security incidents and the associated responses.
- <<Content removed for sample purposes>>
- <<Content removed for sample purposes>>
- <<Content removed for sample purposes>>
- <<Content removed for sample purposes>>

The policy should also include a statement regarding the use of outsourced development and a requirement for equivalent security to be addressed in agreements with third-party developers (see ISO 27002 Clause 14.2.7)."

Document owner and approval

The Information Security Manager is the owner of this document and is responsible for ensuring that it is reviewed in line with the requirements of the management system.

The current version of this document is available to
"Specify which members of staff this document is intended for"

and is published
"Describe the location(s) - electronic and physical - where this document is available"

Its approval status can be viewed in the Master List of Document Approval.