INTLAND SOFTWARE	MS Azure Hosting Policy		Confidentiality Level: Internal
Type: ISMS Documentation	Revision number: 1.0	Created by: Robet Radi – MS Azure Specialist DevOps Approved by: Reka Moksony QA and IT sec. Officer	Valid from: 1st March 2021

Microsoft Azure VM
Cloud Services and Hosting Policy

created by Robert Radi, MS Azure Specialist/Intland DevOps

INTLAND SOFTWARE	**MS Azure Hosting Policy**		Confidentiality Level: Internal
Type: ISMS Documentation	Revision number: 1.0	Created by: Robet Radi – MS Azure Specialist DevOps Approved by: Reka Moksony QA and IT sec. Officer	Valid from: 1st March 2021

Table of contents

<table>
<tr><td>INTLAND SOFTWARE</td><td colspan="2">MS Azure Hosting Policy</td><td>Confidentiality Level: Internal</td></tr>
<tr><td>Type:
ISMS Documentation</td><td>Revision number:
1.0</td><td>Created by:
Robet Radi – MS Azure Specialist DevOps

Approved by:
Reka Moksony QA and IT sec. Officer</td><td>Valid from:
1st March 2021</td></tr>
</table>

Scope

This policy describes information security requirements for Azure VMs, Cloud hosted instances of Intland software applications.

Roles

- Intland Software: Hosting Service Provider (HSP)
- Microsoft Azure: Cloud Service Provider (CSP)
- Purchaser/Customer: User of the tool via hosted/managed environment by Intland on Azure VM

Certifications

Microsoft Azure as Cloud Service Provider:

Microsoft Azure is an ISO27001 certified Cloud Provider. Further Certifications available here: https://docs.microsoft.com/en-us/compliance/regulatory/offering-home

Intland Software as Hosting Service Provider:

Intland Software has ISO 9001: 2015 Certification by TÜV Süd: https://intland.com/wp-content/uploads/2019/09/Certificate_ISO_9001_2015_en.pdf

Intland Software does not have ISO 27001:2013 certification yet, the implementation started October 2020, and planned **to be certified in June 2021.**

The certification Scope defined as:

- ISO 27002:2013 Security Techniques - Code of Practice for information security controls.
- ISO 27017 - Security Techniques - Code of Practice for information security controls based on ISO 27002 for cloud services.

Intland Software has a valid published Information Security Policy by the date November 2020 available here: https://intland.com/wp-content/uploads/2020/12/information-security-policy.pdf

Physical Security

The physical server environment of Azure VMs is managed by Microsoft in Worldwide Data Centers.

(List of Azure regions are available here: Regions and Availability Zones)

The Data Center physical security is the responsibility of the Cloud Services Provider which is described here: Azure physical security.

The Purchaser/Customer has the right to select which Azure region they would like to use for the hosting of Intland's tool if a private instance option is chosen. In a SaaS scenario, the location will be Germany West Central.

Application Security

Intland Software is the tool vendor responsible for the software application as web - application's cybersecurity measurement and features to be implemented. In order to comply with the highest standard Intland implemented **Secure SDLC** process described into internal SOPs.

IT Security

- Intland Software as tool vendor defines and implements standardized **secure builds**.
- Intland software applications are running inside of an Azure Kubernetes cluster on Azure Virtual Machines. Every instance has its own namespace which is protected by a NetworkPolicy. NetworkPolicy restricts the communication within the namespace. Docker containers of the Kubernetes pods are running without root access.
- Only the Intland Software DevOps team have SSH access to the Azure VMs via a bastion host and VPN.
- The Kubernetes cluster is running inside of an Azure Virtual Network. In case of a private deployment no public access is allowed. If SaaS deployment is used, only HTTPs (443), and HTTP (80) are open for public internet. SSH is only accessible from the bastion server, it is protected by private key.
- See the details of the private, and SaaS deployment options here.

Logging

- Azure Monitor is used for logging all changes in the control plane of the Azure system. Application logs are stored in an encrypted format on a storage account, which is only accessible via VPN.
- Data plane logs of the Azure system tracks the activity inside of a given resource component. Access logs, including successful and failed attempts, must include whom accessed which system and at which time.
- Application logs are stored for 1 year/365 calendar days.

Access control

- Every DevOps engineer has an unique Azure account.
- Creation, disabling, or deletion of user accounts are logged.
- Account privileges are assigned and managed by Azure IAM.
- Access control includes system authentication, authorization, provisioning, and revocation for employees and any other Intland Software defined ‘users’.
- Authorized accounts are reviewed only when responsibilities of the account owner are changed.
- Supplier promptly revokes access for former employees. It is part of the offboarding process.
- Passwords are stored in a password manager tool.

Password policy

- A minimum of 8 characters and a maximum of 256 characters.
- Allowed characters:
  - A-Z, a-z, 0-9
  - @ # $ % ^ & * - _ ! + = [ ] { } | \ : ' , . ? / ` ~ " ( ) ;
  - Space
- Unicode chars are not allowed
- Requires three out of four of the following
  - Uppercase characters
  - Lowercase characters
  - Numbers (0-9)
  - Symbols
- Password expires in 90 days
- Remember last password and prevent its usage

Network Security

- Azure Virtual Network contains the Kubernetes cluster, only necessary ports are opened.
- The Bastion server in Azure is protected by key based authentication.

Data Security

- Data is stored in Azure Database for MySQL and on Azure Premium File Shares. Both are encrypted by Microsoft. See:
  - https://docs.microsoft.com/en-us/azure/mysql/concepts-security
  - https://docs.microsoft.com/en-us/azure/storage/files/storage-files-planning#encryption
- Data export is stored on an Azure storage account and only accessible via VPN. Data is compressed and protected by a password
- Daily backups are created and stored in an encrypted format for at least 1 year.
- AES-256 encryption algorithm is used for encryption
- Azure services are only accessible for DevOps team, see "Access control paragraph" for details
- Purchaser data is only used to provide the purchased Service.
- Archival media containing any Confidential Information is retained as required by Applicable Laws and shall be used solely for such purposes.

Incident Management

- Advanced Threat Protection is enabled for the Azure Database for MySQL server. Advanced Threat Protection detects anomalous activities indicating unusual and potentially harmful attempts to access or exploit our database.
- Security Incident Management Process is described in SSP 4.

Cloud Services and Subcontractors

- If involved data is classified by Purchaser as Confidential or Secret, the Supplier will obtain written approval from Purchaser (Director of above) before involving the Third Party.
- Approval of Third Party cloud based IT service is subject to an initial and subsequent periodic security reviews by Purchaser/Customer and such approval may be denied or revoked at any time

Failure to comply with this policy

- In case Intland Software as HSP becomes aware of a non-compliance with security measures in his Deliverables, it must promptly provide the Purchaser/Customer with an analysis of the situation and a remediation plan.
- If the remediation plan is accepted by the Purchaser/Customer, it will be implemented by Intland Software at no cost to the Purchaser and the Supplier must provide proof of remediation plan's sufficiency.
- If non-compliance persists or a remediation plan is not accepted or fails, this will automatically become a non conformity of the service provision.

Effectiveness and Approvals

This document is effective from 1st March 2021.
All previous versions are superseded.

Place of announcement: Stuttgart

The document is created by Robert Radi, MS Azure Specialist/DevOps Team
Signature:

DocuSigned by:
Robert Radi
[illegible]

This document is approved by Reka Moksony, QA and IT Security Officer
Signature:

DocuSigned by:
Reka Moksony
59A6A5E3F21D405...