AWS EC2

Cloud Services and Hosting Policy

INTLAND SOFTWARE	**AWS EC 2** **Cloud services and Hosting Policy**		Confidentiality Level: Internal
Type: ISMS Documentation	Revision number: 1.0	Created by: Sandor Zelei – DevOps AWS, 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">AWS EC 2
Cloud services and Hosting Policy</td><td>Confidentiality Level: Internal</td></tr>
<tr><td>Type:
ISMS Documentation</td><td>Revision number: 1.0</td><td>Created by: Sandor Zelei – DevOps AWS, 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 AWS EC2 Cloud hosted instances of Intland software applications.

Roles

- Intland Software: Hosting Service Provider (HSP)
- AWS: Cloud Service Provider (CSP)
- Purchaser/Customer: User of the tool via hosted/managed environment by Intland on AWS EC2 Cloud.

Certifications

AWS as Cloud Service Provider:

Amazon Web Services is an ISO27001 certified Cloud Provider. Further Certifications available here: https://aws.amazon.com/de/compliance/programs/

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/IEC 27001:2013 Information technology. security techniques. Information security management systems.

- ISO/IEC 27002:2013 Information technology. security techniques. Requirements.
- ISO/IEC 27017:2013 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 AWS EC2 Cloud physical server environment is managed by Amazon Web Services in Worldwide Data Centers.

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

The Data Center physical security if the responsibility of the Cloud Services Provider which is described here: AWS Controls

The Purchaser/Customer has the right to select which AWS region they would like to use for the hosting of Intland's tool.

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 SOP 1.

IT Security

- Intland Software as tool vendor defines and implements standardized **secure builds.**
- Intland software applications are running on **AWS EC2** server inside a docker container without root access.
- Only the Intland Software DevOps team have SSH access to the AWS EC2 via a bastion host and VPN. The personal access rights are managed and documented, supervised via regular audits.
- Production environments and networks are separated from development systems.
    - Production / Test environments are running in AWS,
    - Development environments are running on own on-premise hardware of Intland Software.

    - AWS VPC is used for creating a private network for software application's server, only HTTPS (433) port is open for the public internet. Details here: https://codebeamer.com/cb/wiki/11462356
    - SSH port is also open but only accessible from a bastion server, it is protected by private key and MFA authentication.
    - All installed softwares are approved by the Intland Software's DevOps team. These softwares are installed from official centOS repositories. See: https://wiki.centos.org/AdditionalResources/Repositories
      New software is not possible to install in docker container

Logging

- AWS CloudTrail is used for logging all changes in AWS system, application logs are stored on an encrypted file system, only accessible via Intland Software's VPN.

- Access logs, including successful and failed attempts, must include whom accessed which system and at which time.
- Successful and failed attempts are included with username and time.
- Logs are stored for 1 year/365 calendar days.

Access control

- Every DevOps engineer has an unique AWS account
- Creation, disabling, or deletion of user accounts are logged.
- Account privileges are assigned and managed by AWS 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

- Minimum password length is 8 characters
- Require at least one uppercase letter from Latin alphabet (A-Z)
- Require at least one lowercase letter from Latin alphabet (a-Z)
- Require at least one number
- Require at least one non-alphanumeric character (!@#$%^&*()_+-=[]{}|')

- Password expires in 30 day(s)
- Allow users to change their own password
- Remember last 5 password(s) and prevent reuse

Network Security

- AWS VPC is used for separating clients networks, only necessary ports are opened. See: https://codebeamer.com/cb/wiki/12438698
- The Intland Bastion server is protected by key based authentication and MFA authentication.

Data Security

- Data is stored in AWS RDS and on AWS EBS both servers are encrypted by AWS. See:
  - https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html
  - https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html
- Data export is stored on AWS S3 and only accessible via generated URL
  - Expiration time of the data export link is 1 day
  - Data export is automatically removed after 2 days
  - Data is compressed and protected by a password
- AWS services are only accessible for DevOps team, see "Access control paragraph" for details
- AES-256 encryption algorithm is used for encryption
- Purchaser data is only used to provide the purchased Service.

- Daily backups are created and stored for at least 1 year.
- All data and snapshots are removed upon termination, Purchaser/Customer is notified about the destruction has been accomplished.
- Archival media containing any Confidential Information is retained as required by Applicable Laws and shall be used solely for such purposes.

Incident Management

- AWS GuardDuty is used as state-of-the-art incident detection systems at all times, Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts. Support is available based on agreed SLA Standard or Silver packages.
- Intland Software as HSP notifies the Purchaser/Customer within 1 working day in case a breach of Customer's data is detected.
- Intland Software as HSP uses best efforts to immediately resolve security incidents and inform the Purchaser/Customer of progress and results of corrective actions.
- Intland Software has internal SOPs and SSPs defined to manage security incidents and escalation plans.

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 Sandor Zelei, DevOps Team Lead
Signature:

DocuSigned by:
Sandor Zelei
6C3CB78940F8473...

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

Signature:

DocuSigned by:
Reka Moksony
59A6A5E3F21D405...