RISK ACCEPTANCE FORM

InfoSec Risk Acceptance Ref: MOJ-IS-10

Status: Accepted

Risk Acceptance Title: Application Layer Risk Assessment Tool

Presented On: 22 Feb 2021

Acceptance Date: 22 Feb 2021

Expiration Date: Until Solution is Purchased.

Business Unit:	A-Team
Regulatory Impact:	Non-Compliant with GDPR, PSD2 and PCI DSS
Policy Breach:	Information Security Policies – Mainly A12 Operational Sec, A13 Network A14 Dev Sec.
Linked Enterprise Risk:	REF1234567
Risk Category:	Cyber Security
Risk Owner:	Joe Bloggs
Requested By:	Mr T

Current Risk Assessment (Board Approved 5x5 Matrix):

Inherent Risk Assessment			**Residual Risk Assessment**			**Target Risk Assessment**			**Trend Change**
Likelihood	**Impact**	**Rating**	**Likelihood**	**Impact**	**Rating**	**Likelihood**	**Impact**	**Rating**	↔
Likely	Critical	High	Remote	Critical	Medium	Remote	Critical	Medium	

Risk Issue Details and Risk Acceptance Request:

Currently at COMPANY there is no application vulnerability testing tool to carry out a review for known threats on the application layer. VulnerabilityVector provides this capability. However, there is no budget to purchase the tool (£25,000) to mitigate against any weaknesses on the application code. In addition, a vast number of weaknesses highlighted from the recent IT Naturally Audit found a high number of vulnerabilities.

<u>Summary of Risks to COMPANY</u>

Unauthorised Access leading to Data Leakage
Loss of Service/Availability
Loss of Confidentiality and Integrity
Poor Application Security development controls
Weak access control
Unencrypted data (at rest and in transit)

Risk Issue Cause:
Budget is not available at present to procure a suitable an application vulnerability testing tool such as VulnerabilityVector.

Effect / Impact on the Business:

There is a risk of cyber security vulnerabilities not being identified and remediated in a timely manner, due to inadequate security assessment, authorisation and monitoring controls, leading to financial loss, reputational damage, regulatory intervention, and potential legal action.

Business Justification for the Request:

Budget not available at present

Proposed Action Plan and Compensating Controls:
[Detail the proposed action to address the risk and list the compensating controls that will reduce the risk exposure in the interim]

The following risks should be Mitigated (mitigation action in sub-bullet)

- **Unauthorised Access leading to Data**
  - Leakage (Ensure systems both backend and front are fully updated with the latest patches. Carry out regular vulnerability scanning undertaken.)

- **Loss of Service/Availability**
  - Regular backups are undertaken.

- **Loss of Confidentiality and Integrity**
  - a. Column Encryption will be undertaken using Azure TDE. Operating procedures to be defined.
  - b. Ensure process and awareness raised for all staff handling the service. Including call centre, development, operations, and infrastructure team.

- **Weak access control**
  - Segregation of duties maintained by network access control on active directory. Starters and leavers process to be defined as part of the Infra Cloud Security Strategy / Plan.

- **Unencrypted data (in transit)**
  - Enabling SSL (TLS 1.2) website certificate application.

The following risks should be Accepted

- Poor Application Security development controls
  - A vulnerability scan will not be carried out as Secure Development testing tool VulnerabilityVector is not in place.

Associated Costs / Resources:
[Detail any associated costs or resourcing requirements to manage / mitigate the risk]

APPROVALS

Business Risk Owner: Joe Bloggs
Decision: **[Approve]**
Comments and Conditions:

Signature & Date:

Director Legal, Risk & Compliance: Colonel Hannibel
Decision: **[Approve]**
Comments and Conditions: [Add any comments and/or conditions made by the Approver]

Signature & Date:

Audit & Risk Committee Decision: **[Approve / Decline]**
Comments and Conditions: [Add any comments and/or conditions made by the Audit & Risk Committee]

Chair Signature & Date:

MITIGATION PROGRESS AND RISK REVIEW UPDATE:

[Report progress of mitigation action plan and demonstrate how the risk is continually under review and understood]