LawVu Supplier Security Standards
LawVu Information Security Management System

Version History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Changes made</th>
<th>Changed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>17/01/2019</td>
<td>1.0</td>
<td>Initial Draft</td>
<td>Simon Thomas</td>
</tr>
<tr>
<td>18/01/2019</td>
<td>1.0</td>
<td>Review</td>
<td>Sarah Webb</td>
</tr>
<tr>
<td>07/01/2020</td>
<td>1.1</td>
<td>Review</td>
<td>Sarah Webb</td>
</tr>
<tr>
<td>28/01/2020</td>
<td>1.2</td>
<td>Added security certification requirements</td>
<td>Sarah Webb</td>
</tr>
<tr>
<td>09/10/2020</td>
<td>1.3</td>
<td>Review</td>
<td>Sarah Webb</td>
</tr>
<tr>
<td>30/03/2021</td>
<td>1.4</td>
<td>Review</td>
<td>Sarah Webb</td>
</tr>
<tr>
<td>24/01/2022</td>
<td>1.5</td>
<td>Downgraded classification</td>
<td>Sarah Webb</td>
</tr>
</tbody>
</table>

Review Cycle

These Standards will be reviewed at planned and scheduled intervals at least annually or if significant changes occur, to ensure its continuing suitability, adequacy, and effectiveness.

Purpose

LawVu seeks to maintain the security of our sensitive data and systems whenever they are accessed, processed or managed by external parties. Therefore, the risks to our data and systems from external parties must be quantified – and appropriate controls implemented – before access is granted.

Who These Standards Apply To

These Standards apply to suppliers who provide information services to LawVu. Suppliers are responsible for:

- Adhering to these Supplier Security Standard, or having a clearly published, accepted policy
LawVu Supplier Security Standards
LawVu Information Security Management System

● Participating in all review and audit procedures specified in commercial agreements

Minimum Requirements

The following section sets out the minimum security measures that you must implement.

● You will advise us when staff members or contractors who have access to our systems leave your employment
● Staff and third parties connecting remotely to your systems will authenticate using two factor authentication. This includes remote access to email
● Any LawVu information leaving your offices on a device (e.g. USB, laptop) must be encrypted
● Backups will be taken and stored to ensure the integrity and availability of data and services provided to LawVu
● All IT systems will have security patches applied within a reasonable time after release
● Regular external vulnerability scans of your Internet connections/servers and websites will be performed, and you will resolve any issues rated Medium or above within a reasonable timeframe
● Anti-virus software must be installed on all workstations, laptops and servers
● All staff will undergo regular cyber security training
● You will immediately notify LawVu of any security incidents that have the potential to impact us and provide an incident report within a reasonable timeframe
● You must not share remote access details we have given you with other parties without our permission

We may ask you for evidence that you have met these minimum requirements.

Recommended requirements

The following section sets out the additional security measures that we recommend you implement.

Roles and Responsibilities

● Staff will be aware of their security responsibilities

Accounts

● Staff should only be granted the permissions they need to perform their role
LawVu Supplier Security Standards
LawVu Information Security Management System

- Each user will have an individual, identifiable account. Shared accounts should not be used unless there is no reasonable alternative.
- Administrators will use one account for everyday tasks such as browsing the web and reading email, and a different account for administrative tasks (or the equivalent privileged rights protection for Linux systems).
- Service accounts used in your systems will be individual, use unique strong passwords, and cannot be used to log in via remote access.
- A password policy will be used to ensure strong passphrases are chosen by staff.
- An account lockout policy will be used to prevent password guessing attempts and brute force attacks.
- Unattended screens will lock after a period of inactivity, and the user’s password will need to be entered to unlock the screen.
- Passwords and data will be encrypted using TLS 1.2 or above during transmission over the Internet.
- Password files will be encrypted during storage and protected against unauthorised access, deletion or deciphering.
- Password resets must only be performed by authorised staff.
- New passwords provided to staff must be unique.
- Passwords must not be written down or shared.

Email

- All email sent and received should be scanned for viruses.
- Email anti-spoofing measures (DMARC, DKIM, SPF) must be implemented for email sent and received using your company email domain. Your DMARC policy must be set to quarantine or reject.

Remote Access

- Remote access is only available to authorised staff and third parties.
- Browser based remote access (remote email, remote desktop etc.) will use strong encryption (TLS 1.2 or above).

Mobile Devices

- All mobile devices will have a pin code set for their lock screen.
- All mobile devices will be encrypted.
LawVu Supplier Security Standards
LawVu Information Security Management System

- All mobile devices will have security patches installed within a reasonable timeframe dependent on application compatibility

Data Protection
- All staff will be made aware of your privacy policy and their obligations under the Privacy Act 1993
- Access to LawVu data will be restricted to those staff who require it
- Any passwords you have to our systems will be stored in a secure password manager (such as LastPass or other password vault)

Physical and Environmental Controls
- Servers and other critical equipment must reside in a room or cabinet that is secured from unauthorised physical access

Backup and Recovery
- Backups will not be directly controllable from within your production system, to reduce the risk of malicious corruption or deletion
- Backups on removable storage (tapes etc) will be encrypted

Network and Wireless Communications
- Guest wireless will be on a separate network, with no access to the company network
- All communication over wireless networks will use strong encryption

Change Management
- Change management procedures will be followed and will consider security impacts

Vulnerability Management
- Default passwords will be changed to strong unique passwords when implementing systems and equipment
LawVu Supplier Security Standards

LawVu Information Security Management System

Perimeter and Internet Security

- Internet connections will be protected by a firewall. Laptops will use personal firewalls to provide protection when outside of the office
- Company firewalls will be configured on a default deny basis (for both inbound and outbound traffic)

Websites

- Your website must include reasonable security measures including:
  - Operating systems must be configured according to approved security standards
  - Security patches for the underlying O/S, web server, content management system and any plugins will be installed within a reasonable timeframe of release
  - The website will be secured using strong encryption (TLS 1.2 or above) and must maintain a “B” rating or above on SSL Labs Server Test
  - Administration of the website will be secured using strong encryption and two factor authentication
  - Use of anti-malware software
  - Use of a web application firewall
  - PCI DSS compliant if used to take credit card payments

Information Retention and Destruction

- Upon disposal of computer equipment (workstations, laptops, servers, USB drives and other media), all data and software must be rendered unreadable. This includes printers/copiers that have on-board storage
- Paper files containing confidential information must be securely destroyed

This document has been classified as Internal

Page 5/6
info@lawvu.com | +64 (0)7 808 6165
LawVu Supplier Security Standards
LawVu Information Security Management System

Anti-Virus
- All electronic information (data or software) brought into your network must be scanned for viruses by up to date anti-virus software
- Real-time scanning must be used where feasible

Security Incident Management
- A security incident response plan has been created, and is understood by the IT team and by senior management
- Security incident reports will be created after any incidents, detailing the cause, impact, immediate action taken, further action to be taken, and recommendations on measures to be taken to reduce likelihood and impact
- The incident response plan will be updated as required based on recommendations from incident reports

Security Certifications & Standards
- ISO27001 certification will be maintained and you will provide a copy of your statement of applicability and valid certification on request
- SOC2 Type II reports will be made available on request