Titley SCIENTIFIC

Software Security and Incident Response Policy

POL-003 V1

PURPOSE

This policy outlines the steps Titley Scientific will take to protect user data and address any potential vulnerabilities in our software, including Anabat Insight. Our commitment to security aims to safeguard customer trust and comply with relevant legal and ethical standards.

1. Scope

This policy applies to all instances where data from Anabat Insight, such as user license verification data or anonymous usage data, is transmitted to our servers. Although Anabat Insight primarily operates offline, any breaches or vulnerabilities related to its internet-connected features fall under the scope of this policy.

2. Definition of a Data Breach

A data breach involves any unauthorized access, disclosure, alteration, or destruction of data transmitted by Anabat Insight. Examples of a data breach may include:

- Unauthorized access to license verification data.
- Exposure of anonymous usage data transmitted to the server.
- Exploitation of software vulnerabilities that may compromise user systems or data.

3. Preventive Measures

To prevent data breaches and ensure the security of our systems, Titley Scientific implements the following measures:

- Regular Security Audits: Conducting periodic security audits to identify and address potential vulnerabilities in the software, network, or servers.
- Encryption: Ensuring that all data transmitted between Anabat Insight and our servers, including license verification and anonymous usage data, is encrypted using industry-standard protocols, such as TLS.
- Access Control: Limiting access to sensitive systems and data to authorized personnel only, with robust authentication mechanisms.

4. Vulnerability Management

Titley Scientific is committed to managing software vulnerabilities through:

- Monitoring and Detection: Continuously monitoring for potential vulnerabilities in both the software and server infrastructure using automated tools to detect unusual activity or exploits.
- Reporting: Encouraging users, developers, and third parties to report any discovered vulnerabilities via a dedicated security email (insight@titley-scientific.com).
- Response: Upon detecting a vulnerability, the development team will assess its severity and determine an appropriate response, which may include patching the software and informing affected users.

5. Data Breach Response Plan

In the event of a data breach, Titley Scientific will take the following actions:

- Immediate Containment: The breach will be immediately contained to prevent further unauthorized access. This may involve isolating affected systems or suspending potentially compromised services.
- Assessment: A thorough investigation will be conducted to determine the scope of the breach, identifying the data involved and its potential impact on users.
- User Notification: Titley Scientific does not store personal user information, such as email addresses or contact details, which limits our ability to communicate directly with users regarding breaches. Instead, we will inform users through public channels such as:
  - The "Titley Scientific / Anabat User Community" Facebook group.
  - Our official website.
  - Other social media platforms.
- The notification will include:
  - A description of the data affected.
  - The potential risks involved.
  - Recommended actions for users to protect themselves.
  - Measures we are taking to mitigate the breach and prevent future incidents.
- Reporting to Authorities: If the breach involves personal data, Titley Scientific will notify the appropriate regulatory authorities in line with local data protection regulations, such as GDPR.

6. Post-Breach Actions

After a breach has been contained, Titley Scientific will take the following steps:

- Patch Deployment: If the breach was caused by a software vulnerability, a patch will be developed and released as a priority to address the issue.
- Review and Learnings: A post-breach review will be conducted to identify the root cause and improve security measures. This may involve updating the software, refining protocols, or retraining staff to prevent future breaches.

7. User Responsibility

Titley Scientific encourages users to actively participate in maintaining their software security by:

- Keeping their Anabat Insight software updated to the latest version to benefit from security patches.
- Reporting any suspicious activity or potential vulnerabilities to our security team.

8. Conclusion

Titley Scientific is dedicated to protecting the security and privacy of its users. Through this policy, we strive to minimize the risk of software vulnerabilities and data breaches, ensuring a swift response when issues arise to maintain user trust and data integrity.

Dean Thompson
CEO
17 October 2024