Mobile Application Management Policy

Purpose

invise is a Queensland based, Infrastructure & Security Services business focused on the design and implementation of solutions for the Hybrid Cloud. We pride ourselves on delivering market leading consulting and implementation services that focus on the needs of our clients, ensuring the right outcomes are achieved.

The purpose of this procedure is to provide guidelines for the secure and effective management of mobile applications (apps) within ***invise*** to protect our information assets, against unauthorised access, use, disclosure, disruption, modification, or destruction.

Scope

This Policy applies to all mobile devices (smartphones, tablets, etc.) used by employees, contractors, and third-party vendors of ***invise***. who have access to ***invise***'s information assets, regardless of their location or the device they use.

Responsibilities

The leadership at ***invise*** is responsible for implementing and maintaining this Policy, while all employees, contractors, and third-party vendors are responsible for following it.

Approval and Acquisition of Mobile Apps

- All employees, contractors, and third-party vendors must seek approval from the ***invise*** Leadership before downloading any new app.
- The ***invise*** Leadership will review and approve all apps based on invise ***invise***'s security policies and standards.
- Only approved apps from official app stores (e.g., Apple App Store, Google Play Store) should be used.
- Employees, contractors, and third-party vendors should not install any app that is not approved by the ***invise*** Leadership.

Security Measures for Mobile Apps

- Strong passwords should be used to protect the device and app data.
- Encryption should be enabled on the device to protect sensitive information.
- Sensitive information should not be stored on the device unless it is encrypted.

- Regular backups of app data should be taken to minimise data loss in case of device theft or loss.

App Configuration and Updates

- The ***invise*** Leadership is responsible for configuring all approved apps.
- App updates should be installed promptly to ensure the latest security patches and bug fixes are in place.
- The ***invise*** Leadership should be informed of any issues encountered while using an app.

Device Management

- Lost or stolen devices should be reported immediately to the ***invise*** Leadership.
- Remote wipe capability should be enabled on all devices to protect sensitive information in case of theft or loss.
- All devices should be encrypted and have strong passwords to protect sensitive information.
- Devices should be regularly backed up to minimise data loss in case of theft or loss.

Data Retention and Disposal

- Data stored on mobile devices should be regularly backed up and stored securely.
- When a device is no longer needed, all data should be securely erased before disposal.

Incident Response

- In case of a security incident involving a mobile device or app, the ***invise*** Leadership should be notified immediately.
- The ***invise*** Leadership will lead the investigation and take appropriate action to mitigate the incident.

Review and Revision

This procedure will be reviewed and revised regularly to ensure its effectiveness and alignment with changing security threats and technology.

Conclusion

This policy provides guidelines for the secure and effective management of mobile apps within ***invise***. By following these guidelines, ***invise*** can minimise security risks and protect sensitive information stored on mobile devices.