GENERAL PRINCIPLES

Zingmobile's IT Resources are defined as follows:

HARDWARE: Laptops, Desktops, Servers, Mobile Handsets, Tablets
SOFTWARE: Licensed Work-related Applications, Server–based Applications, Client-based Applications, Mobile Apps, Tablet Apps, Wearable Apps, Bots, Scripts, Source Codes
NETWORKS: Local, Wireless, Mobile, Internet, Accesses
DATA: Financials, Projects, Companies, Customers, Partners
INFORMATION: Documented Drafts, Plans, Blueprints, Patents, Business, Contracts, Confidential Agreements, MoUs, NDAs, Databases
PERSONNEL: Administrators, Developers, Project Managers, Business Development, Managers, Key Appointment Holders, Liaison Officers

These IT resources are provided for the purpose of realising business value for Zingmobile. To meet this end, all users are to adopt the following:

- Adopt individual personal security measures for the IT resources authorised to them
- Ensure up-to-date proper anti-virus and anti-malware software are running
- Protect the integrity, privacy and confidentiality of individual IT resources assigned to them
- Adopt security measures based on assessed IT Security risk levels to mitigate or reduce the threats to the IT resources
- Ensure security software patches are up to date
- Back up and archive the IT resources according to pre-assessed criticality levels
- Ensure that identifications of the IT resources and persons assigned these assets, are kept for security incident evaluations and other legal purposes

LEGAL PRINCIPLES

In the event of any proven violation of the above General Principles, Zingmobile may perform one or more of the actions listed below according to the nature, severity, repetition and assessed financial damage to the affected IT resources:

- verbal or written warning to user(s)
- permanent deactivation or temporary suspension of IT resources assigned to the user(s)
- employment suspension or dismissal of user(s)
- official criminal report lodged against the known or unknown user(s)

Data Protection Policy

Zingmobile adheres to the Singapore Personal Data Protection Act 2012 (PDPA) which is a law that governs the collection, use and disclosure of personal data by all private organisations.

Purpose Limitation
Only use or disclose personal data for the purposes defined as part of the assignment/product/project

Notification
Inform the individuals on the purposes for collection, use and disclosure of their personal data during collection.

Consent
Ensure that consent has been obtained from the individual before collecting, using or disclosure of the personal data. Our mobile application complies with the Google EU consent framework for SDK for Web, iOS & Android. SIM-based application are Non-PII.

Access and Correction
Upon request, provide the personal data of the individual and information on how the individual's personal data has been used or disclosed in the past year. Correct an individual's personal data upon request.

Accuracy
Ensure that personal data is accurate and complete during collection or when making a decision which will affect the individual.

Protection
Keep personal data in your possession secure from unauthorised access, modification, disclosure, use, copying, whether in hardcopy or electronic form.

Retention Limitation
Retain personal data only for business/legal purposes and securely destroy personal data when no longer needed.

Transfer Limitation
Ensure overseas external organisations provide a standard of protection comparable to the protection under the Singapore PDPA

Openness
Make available personal data protection policies and practices to public and employees, including complaint process.

Do Not Call (DNC)
Do not send marketing messages to individuals who have registered in the National DNC registry through voice, text messages or fax unless you have obtained their clear and unambiguous consent or have an on-going relationship.

IT Security Policy

The following Handling Instructions are to be adopted at all times to mitigate against:

- IT Resources Theft
- Malicious/Unintentional externally-based modifications
- Malicious/Unintentional internally-based modifications

Handling of Data In Stasis and In Motion

Minimum of AES 256-Bit encryption must be adopted for all LIVE Production-grade transactional, backup and archival data

Two factor authentications (2FA) must be adopted for:

- SIM transactions in the form of 1024-Bit Public Key (device-side in memory) and 32-Bit Private Key (MD5 Hash)
- Email Accounts (Approved Mobile or Hard or Soft Token Generators)
- All Server Accesses by Administrators (Approved Mobile or Hard or Soft Token Generators)

Additional data protection mechanisms must be documented and put in place for specific products or projects based on requirements specified by the owners of such systems.

Handling of Source Codes & Technical Documentation

- Only Approved, Restricted Permission-based Incoming SSH/Shell access to internal Development, Staging and/or Production Servers from non-corporate networks (especially via internet)

- Only Approved, Restricted Permission-based Outgoing SSH and FTP over VPN connections to Partner/Corporate Servers

- Only Management Reviewed and Approved Access Controls. These accesses are to be reviewed periodically.

- Apache Subversion (SVN) must be adopted for current and historical versions of files such as source codes, web pages, mobile pages and documentation

Additional source code protection mechanisms must be documented and put in place for specific products or projects based on requirements specified by the owners of such systems.

Handling of Logs

Zingmobile's log management processes covers all servers, firewalls, and other IT equipment that generate log files recording all events and historical transactions, including authorised and unauthorised accesses.

This information can provide important clues about suspicious activity affecting Zingmobile's infrastructure from within and without. Log data can also provide information for identifying and troubleshooting equipment problems including configuration problems and potential or recently occurred hardware failures.

To ensure these information are retained for periodical analysis and deeper examinations, the following are to be adopted:

- Logs are to be captured on dedicated servers that are physically displaced from primary servers
- Logs are to be written to read-only media for archival purposes
- Critical logs are to be monitored daily and Nagios alerts activated for non-regular behaviour to be examined in greater detail immediately
- Only authorised and approved users will have access to specific logs under their assigned responsibilities
- All log destructions can only be authorised and approved by Zingmobile Data Protection Office (DPO)

Handling of Passwords

Zingmobile users must adopt the following best practices:

- Minimum of 8 unique characters and increase the minimum password length for more sensitive accounts
- Weak passwords must be auto rejected upon submission by users
- Password resets permitted only with authenticated access privileges/rights (e.g. via mobile, email or token generators)
- All password-enabled accesses must be logged including unsuccessful attempts

IT Security Training

Regular Security Meetings are to be conducted by DPO to review all LIVE production systems involving Customer Data with the intent to address any current or future security issues that may arise from time to time.

Periodic Compliance Reviews

Zingmobile will periodically undergo voluntary scheduled and unscheduled IT Security Compliance Audits/Reviews to ensure that comprehensive aspects governing its security posture is evaluated for compliance and/or further modifications as needed.