***Purpose***

In Express International Group, we strive to assure integrity of all information we disseminate, produce, and manage or store, which is duly handled through sound confidentiality procedures. This policy aims to protect our information assets from any internal, external, deliberate or accidental threats.

***Scope***

This policy shall be adopted by all employees who perform their work using any EIG-related documents or those papers containing any personal data whether related to clients, agents or employees.

In other words, this policy shall be applied to all of EIG personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the organization processes from any source.

The main focus is to adopt:

- the level of information (e.g., sensitive or confidential) that would require secure handling
- the legal and contractual requirements that demand information protection
- identified organizational risks
- cultural aspects

The measures that shall be adopted to secure devices, and media.

To pursue the policy, we shall:

- Ensure that all information, including internal, third party, personal and electronic data, is treated with complete confidentiality;
- Maintain integrity of such information;
- Ensure that our information system and the information contained meet the needs of our core and supporting business operations;
- Comply with all applicable statutory and regulatory requirements;
- Safeguard security of our information assets through effective business continuity management;
- Make information available to staff with minimum disruption;
- Increase staff awareness of information security management through education and training;
- Perform reliable access control to protect our information system against unauthorized access.

***Access Control policy:***

- The following are protected by the use of user name and password:
  - Email, SharePoint, OneDrive
  - Accounting software
- We don't use Remote Desktop.
- We use Email app on Mobiles by giving access permission to WIFI.
- Each Department has access permission to open his files on SharePoint.
- We have firewall in order to prevent unauthorized downloads of any program, games, etc.
- EIG employee access:
  - Upon resignation of the employee, all his access privileges for email, SharePoint and OneDrive are stopped by changing passwords. The new password is given to Top Management in case any data are needed for a period of one year; then his/her email is deleted.
  - Upon transfer from one department to the other, he/she keeps the email but his access permission on Cloud folders (SharePoint and OneDrive) are halted and new one is created for his new department.

***Backup Policy:***

- We use Microsoft Cloud as backup on SharePoint & OneDrive.

- We don't use any removable media except Top Management who are authorized to use it, if needed.

***Policy Updates***

- Windows system is updated automatically.
- Kaspersky is updated automatically on daily basis.
- Firewall is updated when ISAP acknowledges new update.
- Email passwords are changed monthly and upon any cyber-attack.
- For any incidents or data breach (Email- SharePoint – OneDrive), Microsoft is contacted for Support.
- For any ADSL problem, we contact the Service Provider.

***CCTV Policy***

- Cameras are recording 24/7.
- Authorized personnel have access to watch CCTV (President, Vice-President, Director of Operations, HR Manager, IT Manager and, gate Security officers).

***Maintaining Compliance***

- All breaches of information security, actual or suspected, will be reported to and investigated by authorized persons including IT Manager and designated incident investigator;
- Information Technology Manager is responsible for documenting and maintaining the Information Security Management System;
- Information Security documents not limited to policies, procedures and guidelines will be made available in both hardcopy and online format through OneDrive to support the this Policy;
- All managers shall implement the policy within their units and ensure that every staff member adheres to the policy. Any identified issues or areas of weakness shall also be documented and sent by email to President and Compliance department.
- Human Resources department shall impose the relevant disciplinary measure on the employee who is proven to breach this policy.
- Training will be provided when and where required.
- Persistent and repeated breaches of the policy shall be referred to the President, Vice-President, HR Manager and Compliance department.

This policy has been approved by Top Management. It will be reviewed, and if necessary revised, annually to keep up to date.

**Approved by:**

**Jerry Nazzal**
**Group President**