Protection of Personal Information (POPI)
INTERNAL INTERNET/EMAIL/CYBER SECURITY POLICY

This Policy document is for internal usage by all employees and consultants of HONEY FASHION ACCESSORIES (which is defined in the organization's DATA PRIVACY POLICY) and all employees and consultants have read through this internal Policy, were afforded an opportunity to ask questions and have acknowledged acceptance of the terms. HONEY FASHION ACCESSORIES recognize that ongoing training will be required to ensure that employees and consultants are empowered in terms of cyber risks and best practices which may ensure risk mitigation of HONEY FASHION ACCESSORIES 's data subjects' information being breached.

1. Acceptable use of HONEY FASHION ACCESSORIES' Internet Facilities

The purpose of these rules below is to direct all employees and consultants of HONEY FASHION ACCESSORIES in the acceptable use and security of HONEY FASHION ACCESSORIES' Internet Facilities. These rules contain directions for employees and consultants, indicating both acceptable and unacceptable Internet use with the aim of controlling employee behavior and actions that contribute to HONEY FASHION ACCESSORIES' Internet risks, while maximizing the benefits gained by HONEY FASHION ACCESSORIES through Internet usage. As the software, hardware and computer network is the property of HONEY FASHION ACCESSORIES it reserves the right to keep HONEY FASHION ACCESSORIES and its systems secure through monitoring electronic information and regular checks on the system.

1.1. HONEY FASHION ACCESSORIES' Management will establish a periodic reporting requirement to measure the compliance and effectiveness of this policy.
1.2. HONEY FASHION ACCESSORIES' Management is responsible for implementing the requirements of this policy, or documenting non-compliance via the method described under exception handling.
1.3. HONEY FASHION ACCESSORIES' Managers, in cooperation with the Information Officer, are required to train employees and consultants on policy and document issues with Policy compliance.
1.4. All of HONEY FASHION ACCESSORIES' employees and consultants are required to read and acknowledge the reading of this policy by signing it.

The repercussions of misuse of HONEY FASHION ACCESSORIES systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g. computer viruses), legal and financial penalties for data leakage and lost productivity resulting from network downtime. In order to ensure that HONEY FASHION ACCESSORIES' IT systems are not misused, everyone who uses or has access to HONEY FASHION ACCESSORIES systems must meet the following five high-level IT Security requirements:

- Information must be protected against any unauthorized access;
- Confidentiality of information must be assured;
- Integrity of information must be preserved;
- Availability of information for business processes must be maintained;
- Compliance with applicable laws and regulations to which HONEY FASHION ACCESSORIES are subject must be ensured.

Employees and consultants will only be given sufficient rights to all systems to enable them to perform their job function and in terms of HONEY FASHION ACCESSORIES' EMPLOYEE CODE OF CONDUCT. User rights will be kept to a minimum at all times. Employees and consultants must report any weaknesses in HONEY FASHION ACCESSORIES' computer security to the appropriate security staff. Weaknesses in computer security include unexpected software or system behavior, which may result in unintentional disclosure of information or exposure to security threats. Employees and consultants must report any incidents of possible misuse or violation of this Acceptable Use Policy to the Information Officer. Employees and consultants must not attempt to access any data, documents, email correspondence, and programs contained on HONEY FASHION ACCESSORIES' systems for which they do not have authorization.

Systems administrators and authorized users must not divulge remote connection modem phone numbers or other access points to HONEY FASHION ACCESSORIES' computer resources to anyone without proper authorization in writing. Employees and consultants must not share their account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes. Employees

and consultants must not make unauthorized copies of copyrighted software or software owned by HONEY FASHION ACCESSORIES. Employees and consultants must not use non-standard shareware or freeware software without the approval from Management. Employees and consultants must not purposely engage in activity that may harass, threaten or abuse others or intentionally access, create, store or transmit material that HONEY FASHION ACCESSORIES may deem to be offensive, indecent or obscene, or that is illegal in terms of applicable legislation.

Employees and consultants must not engage in activity that may degrade the performance of Information Resources; deprive an authorized user access to HONEY FASHION ACCESSORIES' resources; obtain extra resources beyond those allocated; or circumvent HONEY FASHION ACCESSORIES' computer security measures. Employees and consultants must not download, install or run security programs or utilities such as password cracking programs, packet sniffers, or port scanners that reveal or exploit weaknesses in the security of HONEY FASHION ACCESSORIES' computer resources unless approved by Information Officer. HONEY FASHION ACCESSORIES' Information Resources must not be used for personal benefit, political activity, unsolicited advertising, unauthorized fund raising, or for the solicitation of performance of any activity that is prohibited by relevant legislation.

Access to the Internet from home based computers or computers owned by HONEY FASHION ACCESSORIES, must adhere to all the rules contained within the HONEY FASHION ACCESSORIESEMPLOYEE CODE OF CONDUCT and additional rules which may be communicated to employees and consultants from time to time. Employees and consultants must not allow family members or other non-employees and consultants to access non-public accessible computer systems of HONEY FASHION ACCESSORIES. Employees and consultants must not attempt to change the configuration of desktop computers and notebooks. All configuration changes must be handled by the IT department, for example upgrading operating systems, changing Windows settings, installing new software or systems, and installing modems, memory or storage upgrades. Employees and consultants of HONEY FASHION ACCESSORIES may not send or publish confidential and private material of HONEY FASHION ACCESSORIES (internal memos, policies, etc.) on any publicly accessible or external Internet computer of HONEY FASHION ACCESSORIES unless the owner of the information has first approved the publication of these materials. Employees and consultants should not transmit confidential information, information of HONEY FASHION ACCESSORIES, copyrighted materials, or any trade secrets of HONEY FASHION ACCESSORIES over any public computer system or network unless properly protected through encryption methods.

Occasional private use of HONEY FASHION ACCESSORIES' Internet facilities is allowed under the following enhanced conditions in addition to the conditions contained in the EMPLOYEE CODE OF CONDUCT:

1.5. Occasional and very short personal email communications by users are acceptable provided that they do not interfere with the users work and comply with the guidelines of this policy at all times. If the user is not sure whether a personal communication complies with the requirements of this policy, the prior authorization of the user's superior must be obtained before such messages are sent.
1.6. Personal use of HONEY FASHION ACCESSORIES' Internet facilities must be kept to a minimum. Personal usage must not interfere with the user's work and such usage must comply with the requirements of this policy at all times.
1.7. Incidental use must not result in direct costs to HONEY FASHION ACCESSORIES, cause legal action against, or cause embarrassment to HONEY FASHION ACCESSORIES.
1.8. Incidental use must not interfere with the normal performance of an employee's work duties.
1.9. Storage of personal email messages, voice messages, files and documents within HONEY FASHION ACCESSORIES' computer resources must be nominal.
1.10. HONEY FASHION ACCESSORIES' Management will resolve incidental use questions and issues using these guidelines in collaboration with the Information Officer, HR Manager and the Line Manager/Supervisor.

Every user of HONEY FASHION ACCESSORIES' IT systems is responsible for exercising good judgment regarding reasonable personal use. HONEY FASHION ACCESSORIES' Director(s) and Management will commit to the on-going training and education of staff responsible for the administration and/or maintenance and/or use of HONEY FASHION ACCESSORIES' Internet facilities.

HONEY FASHION ACCESSORIES' Director(s) and Managers will establish a formal review cycle for all Acceptable Use initiatives.

Any security issues discovered will be reported to the Information Officer.

2. Ownership

Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of HONEY FASHION ACCESSORIES are the property of HONEY FASHION ACCESSORIES and employee use of these files is neither personal nor private. The Information Officer may access all such files at any time

without knowledge of the user or owner. HONEY FASHION ACCESSORIES' management reserves the right to monitor and/or log all employee use of HONEY FASHION ACCESSORIES' Information Resources with or without prior notice

3. IT Access Control

HONEY FASHION ACCESSORIES shall ensure that logging into the IT system and software packages is password controlled and shall exercise all caution in allowing unauthorized access to the password. The password shall be reviewed from time to time but in particular where GOOGLE based products are used and linked (such as Facebook, Whatsapp and GMAIL based domains).

Users will be granted the minimum access required to perform their specific tasks. Granting access levels to resources shall be based on the principle of least privilege, job responsibilities, and separation of duties. The level of minimum access requires the recommendation of the user's manager, and the evaluation of the Information Officer. The Information Officer has final determination as to the level of a user's access for their system.

Each individual assigned a user account and password is responsible for the actions taken under said account, and must not divulge that account information to any other person for any reason.

Management access to user accounts will be limited to business purposes only, such as during an emergency or contingency situation, cases of extended user absence, or user abuse of HONEY FASHION ACCESSORIES' information resources. HONEY FASHION ACCESSORIES' management will implement procedures to immediately cancel account access and physical access for users whose relationship with HONEY FASHION ACCESSORIES have concluded, either on friendly or unfriendly terms.

Access points for remote computing devices shall be configured using necessary identification and authentication technologies to meet security levels of physically connected computers.

The rules herein contain apply to all information resources, systems, and technology and to all users of these resources, systems and technology within HONEY FASHION ACCESSORIES' operating environment or connected to HONEY FASHION ACCESSORIES' information infrastructure.

3.1. HONEY FASHION ACCESSORIES 's Email Rules

HONEY FASHION ACCESSORIES acknowledge that most of its communications are conducted via email and instant messaging (IM). Given that email and IM may contain extremely sensitive and confidential HONEY FASHION ACCESSORIES information, the information involved must be appropriately protected. In addition, email and IM are potentially sources of spam, social engineering attacks and malware, so HONEY FASHION ACCESSORIES must be protected as completely as possible from these threats. The misuse of email and IM can post many legal, privacy and security risks, so it is important for users to be aware of the appropriate use of electronic communications.

HONEY FASHION ACCESSORIES provide employees and consultants with electronic communication tools, including an e-mail system. This email policy, which governs employee use of HONEY FASHION ACCESSORIES' e-mail system, applies to e-mail use at HONEY FASHION ACCESSORIES' premises as well as remote locations, including, but not limited to, employee homes, airports, hotels, and client and supplier offices. HONEY FASHION ACCESSORIES' e-mail rules and policies apply to full-time employees and consultants, part-time employees and consultants, independent contractors, interns, consultants, suppliers, clients, and other third parties. Any employee who violates HONEY FASHION ACCESSORIES' e-mail rules and policies is subject to disciplinary action, up to and including termination.

HONEY FASHION ACCESSORIES reserve the right to monitor, inspect, copy, review, and store any and all employee's e-mail use at any time and without prior notice. In addition, HONEY FASHION ACCESSORIES may monitor, inspect, copy, review, and store any files, information, software, and other content created, sent, received, downloaded, uploaded, accessed, or stored through HONEY FASHION ACCESSORIES' e-mail system. HONEY FASHION ACCESSORIES reserve the right to disclose e-mail information and images to regulators, courts, law enforcement agencies, and other third parties without the employee's consent.

Users of HONEY FASHION ACCESSORIES' email system are prohibited from using email to:

3.1.1. Send, receive, solicit, print, copy, or reply to text, images, or jokes that disparage others based on their race, religion, colour, gender, sex, sexual orientation, national origin, veteran status, disability, ancestry, or age.

3.1.2. Send, receive, solicit, print, copy, or reply to messages that are disparaging or defamatory.

3.1.3. Spread gossip, rumours, or innuendos about employees and consultants, clients, suppliers, or other outside parties.

3.1.4. Send, receive, solicit, print, copy, or reply to sexually oriented messages or images.
3.1.5. Send, receive, solicit, print, copy, or reply to messages or images that contain foul, obscene, disrespectful, or adult-oriented language.
3.1.6. Send, receive, solicit, print, copy, or reply to messages or images that are intended to alarm others, embarrass HONEY FASHION ACCESSORIES negatively impact productivity, or harm morale.

Unless authorized to do so, employees and consultants are prohibited from using e-mail to transmit confidential information to outside parties. Employees and consultants may not access, send, receive, solicit, print, copy, or reply to confidential or proprietary information about HONEY FASHION ACCESSORIES, its employees and consultants, clients, suppliers, and other business associates. Confidential information includes, but is not limited to, client lists, credit card numbers, identification numbers, employee performance reviews, salary details, trade secrets, passwords, and information that could embarrass HONEY FASHION ACCESSORIES and its employees and consultants if the information were disclosed to the public.

All messages communicated on HONEY FASHION ACCESSORIES' Internet and e-mail system must contain the employee's name. No e-mail or any other electronic communication may be sent which hides the identity of the sender or represents the sender as someone else. All emails sent must include the email signature of the sender. Emails with attachments sent by employees and consultants may not exceed the limit as prescribed by the Information Officer. The disclaimer as prescribed by the IT department must be used at the end of all email messages.

The purpose of these rules is to ensure that information sent or received via these HONEY FASHION ACCESSORIES 's IT systems is appropriately protected, that these systems do not introduce undue security risks to HONEY FASHION ACCESSORIES and that users are made aware of what HONEY FASHION ACCESSORIES deem as acceptable and unacceptable use of its email and IM.

3.2. HONEY FASHION ACCESSORIES 's Rules related to handheld devices

Many users do not recognize that mobile devices represent a threat to IT and data security. As a result, they often do not apply the same level of security and data protection as they would on other devices such as desktop or laptop computers. This policy outlines HONEY FASHION ACCESSORIES' requirements for safeguarding the physical and data security of mobile devices such as smartphones, tablets, and other mobile devices that PC's and Notebooks.

3.2.1. Users of handheld devices are expected to diligently protect their devices from loss and disclosure of private information belonging to or maintained by HONEY FASHION ACCESSORIES.
3.2.2. In the event of a security incident or if suspicion exists that the security of HONEY FASHION ACCESSORIES 's systems has been breached, HONEY FASHION ACCESSORIES shall be obliged to notify the IT support immediately especially when a mobile device may have been lost or stolen.

The IT support must ensure that all employees and consultants using devices falling into the category of "handheld devices" have acknowledged this security policy and the associated procedures before they are allowed to use corporate services using handheld devices. The IT support must ensure that handheld devices and their users comply with this security policy and all security policies as stipulated by HONEY FASHION ACCESSORIES. Any employee found to have violated this policy is subject to disciplinary action, up to and including termination. In a general sense, all users are required to use their common sense in order to act in the best interest of HONEY FASHION ACCESSORIES, its assets and its services. In case of doubt, users must contact the IT support to clarify a given situation.

HONEY FASHION ACCESSORIES will arrange, where necessary, training in respect of the handheld devices in as far as:

Password protection, how to deal with social engineering attacks, proper protection of devices, locking the device, preventing the use of systems by unauthorised users, protecting devices from loss or theft, ensuring the information on a handheld device is absolutely necessary, ensuring the information on a handheld device is also stored on HONEY FASHION ACCESSORIES' network where it is regularly backed up, how to encrypt sensitive information.

Users must not modify security configurations without request to and approval by the IT support of management of HONEY FASHION ACCESSORIES. Failure to comply with this rule will engage disciplinary procedures. Unauthorised actions include but will not be limited to: installing and/or using unauthorised applications or services, removing root certificates from certificate stores, conducting any careless actions leading to an interruption or service, disabling security features.

3.3. Anti-virus rules

These rules apply to all of HONEY FASHION ACCESSORIES' computers that are PC-based or utilize PC-file directory sharing. This includes, but is not limited to, desktop computers, laptop computers, file/ftp/tftp/proxy servers.

All of HONEY FASHION ACCESSORIES' PC-based computers must have HONEY FASHION ACCESSORIES' standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Where applicable HONEY FASHION ACCESSORIES management is responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free.

Any activities with the intention to create and/or distribute malicious programs into HONEY FASHION ACCESSORIES' networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the Acceptable Use Policy.

Users must not attempt to remove viruses themselves. If a virus infection is detected, users must disconnect from HONEY FASHION ACCESSORIES' networks, stop using the infected computer immediately and notify the IT department.

Users must be cautious of e-mail attachments from an unknown source as viruses are often hidden in attachments. If a virus is suspected the attachment must not be opened or forwarded and must be deleted immediately.

Users are discouraged from attempting to remove viruses themselves. If a virus infection is detected, users are expected to disconnect from HONEY FASHION ACCESSORIES' networks, stop using the infected computer immediately and notify the Information Officer.

This Policy document has been adopted together with the DATA PRIVACY POLICY for HONEY FASHION ACCESSORIES and all employees and consultants undertake to abide to the rules herein contained where ever possible and the HONEY FASHION ACCESSORIES' Information Officer confirms that this Policy has been circulated to all employees and consultants.

HONEY FASHION ACCESSORIES undertake further to work with its internet managers to allow for continuous updating of rules and internal processes from time to time.

INFORMATION OFFICER

_____

DATE: _____