DOB ENTERPRISES PTY LTD

DOB Equipment and Software Policy
IMS-503-00-POL

Revision History

Date	Rev	Modified By	Changes Made, Review History	Reviewed by	Approved by
16.04.18	0	Sunette Opperman	Creation	S Rupert	S Rupert

Purpose of this policy

This policy is to provide rules and guidelines specific to acceptable use of all Company equipment made available to employees and contractors of the Company. This includes, but is not limited to: Personal Computers (PC's), laptops, mobile phones, printers and any other Company equipment an employee is given access to, both internally and externally.

The policy has been designed to protect the confidentiality, integrity and availability of data and resources using Company equipment, computer networks and smartphones.

Definitions

Equipment - Pursuant to this Policy, equipment is classified as any device or software that is made available to an employee or a contractor to perform their duties. This includes mobile phones, PC's at the office, laptops, tablets, terminals and any other device that is deemed necessary.

Company Network - The internal company network that is controlled and maintained by DOB Enterprises.

Software – Encompasses all functions that can be performed on Company equipment, as defined above.

Backup - A process in which data that a user has generated is replicated in a remote location to preserve data in the event of equipment failure, disasters or user errors.

Remote Access - Denotes the ability to access Company information and software away from the Company's premises – i.e. from home, customer site, overseas etc.

Username and Password - A unique identified given to an employee or contractor that denote permission to access certain functions relevant to their position.

Monitoring - The ability of the Company to access all information transmitted on the Company Network.

Authorised Use

Access and Use of I.T. Resources, Equipment and Software Policy applies to all users of the Company's equipment including employees, agents and contractors.

The Company's equipment and access to the network are to be used only by persons authorised by the Company.

Authorised users are those who are issued a username and password by the Company. The username and password will grant the user access to information based on his/her job requirement and security level authorisation.

Issue of equipment

Upon employment by the company, the employee will be provided with the equipment required to perform the required duties, as deemed by the Director.

Depending on the position, this may include issue of a portable company device, such as a laptop, mobile phone or tablet, that the employee will become the custodian of, and be responsible for as outlined by this Policy.

The employee, if required, may be given access to a P.C. that remains on company premises after hours.

For the employee to be granted a username and password, the Director will arrange with Management to ensure that the account is created in a timely manner.

Regular equipment reviews will be conducted by management.

Software

All equipment provided by the company will contain software deemed necessary for the employee to perform his/her duties.

Any additional software requirements must be approved by the Director, who will assess the requirement and ensure that additional software installed adheres to Company Policy, including licencing requirements.

Company Network

Most equipment provided by the Company, will have direct access to the Company's network and utilise the Company's infrastructure. As a core asset of the Company, the network contains vital information required for the operation of the business. As such, it is the responsibility of all staff to maintain the integrity of information and security of the network always.

It is each employee's responsibility to ensure their practices protect the Company's interests always. The following section of the Policy outlines major guidelines, however any action that can be deemed inappropriate must be avoided. The Company has an obligation that all relevant laws are complied with.

The Sex, Race, Age and Disability Discrimination Acts prohibit sexual harassment, racial vilification and other forms of unlawful discrimination which could occur through usage of Company issued equipment, including email and internet usage.

The following use of **email and internet** is prohibited:

- Defaming, harassing, abusing or otherwise offending another person.
- Accessing, downloading, storing or transmitting material of an offensive nature (for example sexually explicit pictures, or racially discriminatory jokes).
- Sending offensive comments based on a person's gender, age, sexuality, race, religious background, disability or appearance.

Using Company issued equipment or software for illegal purposes or a manner that would expose the Company to investigation or inquiry by the Police or other Government Agencies (For example pornographic material).

Accessing illegal or inappropriate internet sites (for example pornographic, file sharing, torrenting or pirate websites).

Using Company issued equipment with a built-in camera to perform any activity which may be considered illegal or offensive.

Accessing, saving or distributing material that could cause damage or harm the reputation of the Company or material that could be misleading or deceptive.

Attempting to obscure the origin of any message or otherwise disguise user identity.

Unauthorised transmission of sensitive and confidential information belonging to the Company.

Knowingly obtaining, permitting or assisting unauthorised access to information or damaging, deleting, inserting or otherwise altering such information.

Infringing copyright, software licences or making personal profit or private gain by using someone else's
intellectual property including software, programs, data, music, pictures etc.

Breaching the Company's Social Media Policy.

Actions that could reasonably be expected to directly or indirectly cause strain on any computing facilities, or interference with others' use of the system. This includes but is not limited to:

(widespread distribution of unsolicited email), Letter Bombing (repeatedly sending the same email to one or more recipients) or sending/forwarding chain letters.

Further to the above, the following actions pertaining to the Company network are **strictly prohibited**:

- Unauthorised access to the Company network (i.e. hacking), attempting or assisting someone else to 'hack', circumvent, bypass or disable security access controls on any Company equipment.

- Attempting, or assisting someone else to "crash" or unnecessarily slow the computer systems or networks including unauthorised use, alteration or destruction of computing resources.
- Attempting, or assisting someone else to read, copy, alter or delete another users' files or electronic mail without their consent, even if the operating system allows this. The Company has the right to access user files and email as specified in the section 'Monitoring and Privacy' within this policy document.
- Executing any form of network monitoring which will intercept or receive data not intended for that user (for example sniffing), port scanning or security scanning, adding, removing or modifying network headers or other identifying information (spoofing).
- Attempting to modify or reconfigure hardware or software on Company issued equipment or network.
- Copying, installing or using any software or data files in violation of applicable copyright or licence agreements.
- Creating, installing or knowingly distributing a computer virus, trojan or another malicious program.
- The downloading and transmission of games, movies, screen savers and other executable files is prohibited unless for a business use or as authorised by Management.
- Using a system other than those provided by the Company to store files relating to the Company.
- Exporting software, technical information, encryption software or technology in violation of international regional export control law.
- Attempting to impersonate another person by using forged headers or other identifying information or using any type of 'anonymiser' or any other means to mask, hide or modify your identity.
- Facilitating use or access by non-authorised users including sharing your username and password.

Employees must exercise caution with any unexpected or unusual emails, even if the message is from a known source.

Emails with an attachment from an unknown source must not be opened. All suspicious emails must be reported to your Manager.

Remote access

This section of the Policy applies to persons that either are custodians or Company equipment or have remote (i.e. Offsite) access to any part of the Company's network and infrastructure. Remote access users must ensure that their remote access connection is given the same consideration as the user's on-site connection to the Company's computer network.

Remote access users not using Company provided equipment must install the most up-to-date anti-virus software. The anti-virus software must be running always and must be approved by the Company.

Computer equipment intended to be used for remote access must be approved by management.

“Split-tunnelling” is strictly prohibited. Remote access users must not be connected to any other network while connected to the Company’s network, apart from personal networks that are under complete control of the remote access user.

User Responsibility

Custodians of Company I.T equipment (e.g. laptops, portable devices) are responsible for the physical security of the equipment they’ve been provided.

Your equipment, when not physically with you, should be stored in a secure place, either at work or at home. Motor vehicles do not constitute a secure place and should only be used when you are unable to take the device/equipment with you.

If you have no alternative but to leave a piece of equipment in the car, they must be stored in the vehicle’s boot. If you are entering a car park, the equipment must already be stored in the boot. Do not place equipment in the boot after entering car park, as you risk being observed doing so and increase chances of equipment being stolen.

Equipment is likely to have confidential information relating to the Company stored on the hard disks. Therefore, when visiting customer or non-affiliated premises, the equipment is not to be left unattended at any time.

When on Company premises, the equipment must still be in a secure location such as an office.

Users are responsible for maintenance and condition of their devices and are responsible for notifying management if their equipment needs replacement or repairing. They are also responsible for returning equipment in good working order similar to as received.

Passwords

Security of the Company’s system is achieved through several independent security levels, one of which is the issuing of passwords to employees. Unique passwords are issued to provide employees with access that they require to perform their duties. Conversely the access granted will restrict access to areas of the system that is not required

It is the responsibility of each employee to preserve the secrecy of their password and to ensure that no other staff member has access to that password. An employee

must only use their own password and should not, under any circumstance, attempt to identify another employee's login information for any part of the Company's system.

For security purposes, domain passwords will expire and will require a new password at least every 6 weeks. The equipment will either prompt you with a 'password expired' screen when attempting to log in, or alternatively you can change the password manually by pressing CTRL + ALT + DELETE and selecting the 'Change a Password' option. If you believe your password has been compromised, you should change it immediately.

In the event you have forgotten your password, you can have it reset by contacting the **Head Office at 02 6584 0033.**

The following guidelines are to be used when selecting your password to ensure security:

Select passwords that are easy to remember but not obvious – i.e. do not repeat your username, surname, children's names or pets.

Never write your password down.

Use at least 6 characters, with a combination of lower and upper-case letters, as well as a combination of alpha, numeric and symbols.

Passwords should be easy to type quickly, so another person will not be able to follow or replicate by watching the keyboard.

Never give your password to anyone.

Personal Use

The Company will tolerate occasional personal use of issued equipment in the following circumstances:

- Where the use takes place outside employee's usual work time.
- Where it does not incur any additional expense to the Company.
- Where it is infrequent and brief.
- Where it does not breach this Policy.

Any personal use beyond the guidelines set out in this Policy must be authorised by your Manager. Excessive personal use may lead to disciplinary action and/or the revocation or suspension of access.

Employees must not map their private email addresses to the Company's software (e.g. Outlook) and/or equipment.

Monitoring and Privacy

The Company has the right to monitor and access all aspects of its computer system including email and the internet usage by employees, across all Company issued devices.

A log of all emails received and transmitted, as well as internet sites visited is kept by the Company for record purposes.

Employees do not have a right to privacy with respect to their email and internet usage while on the network or using Company issued equipment.

Legitimate reasons for monitoring and access include but are not limited to the following:

- Ensuring that this Policy is being adhered to.
- Ensuring that there is no illegal or improper use of email, internet or Company issued equipment.
- Investigating complaints from other employees, clients, customer or Government agencies.
- Assessing the level of personal usage.
- Accessing or retrieving emails that may have been deleted.
- Retrieving necessary data from Company equipment relating to former employees.

The Company does not intend to read emails or monitor internet usage daily. Monitoring will occur for any of the above reasons, including where the Company reasonably believes an employee has committed a disciplinary or offence, is in breach of this Policy and/or where the Company is legally obligated to do so.

Breaches and Disciplinary Action

As is the case with all the Company's policies, if you do not comply with this Policy you may face disciplinary action.

If the breach involves breaking the law, you may also be personally liable. The Company may report any breaches of State or Federal laws to the relevant government agency.

Disciplinary action may result in revocation or suspension of your access. It may also include a verbal or written warning.

Serious or repeated breaches of this Policy may lead to instant dismissal.

This Policy has been put in place to protect the Company and its employees from liability. If the Company incurs any liability because of an employee not complying with this Policy, the employee will be liable for any damages or other liability arising out of the breach.