BARDAVCOL

CP-18

COMPUTER SECURITY POLICY

Controlled Copy No ###

CONTENTS LIST

COMPUTER SECURITY POLICY

1.0 INTRODUCTION

POLICY OBJECTIVES

2.0 RESPONSIBILITY

3.0 PURCHASE OF HARDWARE AND SOFTWARE

4.0 SOFTWARE

5.0 HARDWARE

6.0 SECURITY

7.0 ELECTRONIC MAIL

8.0 INTERNET USAGE

9.0 VIRTUAL PRIVATE NETWORK

10.0 REMOTE ACCESS

11.0 SMART PHONES, TABLETS AND MOBILE DEVICES

12.0 NON COMPLIANCE

COMPUTER SECURITY POLICY

1.0 INTRODUCTION

Bardavcol Pty Ltd provides information technology (IT) equipment and software for its employees to use in accordance with the performance of their specific duties and to enable Bardavcol Pty Ltd to operate in the most efficient and effective manner.

In order to ensure that Bardavcol Pty Ltd, its employees and external consultants are protected from legal liability arising from breaches of discrimination and other laws, the acceptable standard of behaviour and usage by all employees in relation to the IT equipment and software is outlined below.

For the purposes of this Policy, IT equipment includes servers, computers, laptops, network hardware, smartphone and tablets along with any software and systems required for these devices.

Breaches of the Computer Security Policy BAR-SP-02 will result in the employee being subject to disciplinary action, and in serious cases termination of employment.

POLICY STATEMENT

Policy Objectives

This policy details the expectations of Bardavcol and the responsibilities of all computer users. This policy is not designed to restrict computer users from performing the different aspects of their job efficiently and effectively.

All computer users are encouraged to play an active role in ensuring the security of computer systems by understanding and complying with the Bardavcol Computer Security Policy. If the policies are unclear or conflict with business objectives it is the user’s responsibility to contact the Applicable Manager/Office Manager immediately.

It is the responsibility of each Applicable Manager to ensure that the policy is complied with and report any breaches to the Office Manager immediately.

Scope

This policy will be reviewed and updated (if required) on a yearly basis. The policy includes, but is not limited to:

- Personal Computers including portable computers and mobile devices (eg. notebooks / laptops smartphones etc);
- Local area networks and servers;
- Telecommunications and data communication facilities; and
- Data, applications software and operating systems residing on Computers or local area networks and servers.

Policies

Computer users are to comply with the following policies:

- Responsibility
    - All computer users shall report any known or suspected breaches of this policy to the Office Manager.
    - Hardware and software shall not be purchased by individual users or departments. All computer requirements shall be communicated to the Office Manager.
- Software
    - Software shall only be installed (or arranged to be installed) by the Office Manager only.
    - Unauthorised software is not permitted to be loaded onto any Bardavcol computer.
    - Games and other entertainment software are not permitted on Bardavcol computers.
    - Virus protection software shall be installed on all personal computers.
    - Computer users shall scan all files originating from external locations prior to use.
- Hardware
    - Only authorised Bardavcol hardware (authorised by the Office Manager) shall be connected to our network.
    - Reasonable steps shall be taken to protect hardware from loss or damage.
    - Laptop / notebook computers / smart phones shall be physically secured at all times.
    - Any actions undertaken by the assigned user which may contribute to the theft or damage of any company supplied personal computer may result in the user being personally liable for its replacement.
- Security
    - Users are responsible for the security of their username and password and for the files that can be accessed by this password.
    - Users are accountable for activities performed under their username.
    - All Computers belonging to Bardavcol shall have password protection and screen saver password protection activated.
    - Network passwords shall follow the complexity guidelines to ensure that they can not be easily guessed and should be changed every 90 days.
    - All sensitive, valuable or critical information held on offsite computers shall be backed up daily and appropriately secured (remote users are required to save valuable information on external storage e.g. USB stick to ensure a safe ~~to~~ back up).

  - All backup media shall be stored in a secure, safe place.
  - Only authorised personnel are permitted to access any Bardavcol computer workstations and laptops.
- Electronic Mail (E-mail)
  - E-mail is a productivity tool and shall be used for business activities only.
  - E-mail correspondence shall comply with standard Bardavcol circulation and filing requirements.
  - Staff are required to maintain the highest standard of business etiquette within e-mail.
  - All e-mail shall include the disclaimer contained in section 7 of the policy guidelines.
  - All external emails are run through Audit In and Audit Out which is monitored by the receptionist
- Internet Usage
  - Corporate Internet accounts shall be utilised for business purposes only and access to information which is prohibited by federal or state legislation is not permitted.
  - No social media or purchasing sites are to be accessed with Bardavcol laptops/desktops/smart phones (eg Facebook, Twitter, Instagram, Ebay etc)
- Virtual Private Network
  - Only approved users and authorised third parties may utilise access to Bardavcol's VPN .
  - It shall be the responsibility of authorised VPN users to ensure that unauthorised users are not allowed access to Bardavcol's internal networks.
- Remote Access
  - Only approved users and authorised third parties may access Bardavcol's network via Remote Access.
  - Remote users shall not disclose their passwords to anyone..
  - Computers shall not be left unattended while remotely accessing the network and should activate the timer on their screensaver to a minimum of 4 minutes.
- Non Compliance
  - All breaches in the Computer Security Policy must be reported to the Office Manager and the users Applicable Manager.

POLICY DETAIL

2.0 RESPONSIBILITY

All staff, temporary staff, contractors and consultants must be authorised to use Bardavcol computing resources and must understand and comply with this policy. All authorised users are required to sign an acceptance of this policy statement.

All information on Bardavcol's computers and network is company property and is protected by intellectual property rights. All computer users shall be assigned an account on the network, and are not permitted to access or seek to access information for the purpose of inquiry or modification that is outside the requirements of their job function. User's activities, including Internet usage and external emails, will be monitored and reviewed.

It is the responsibility of each Applicable Manager to ensure that this policy is complied with. Applicable Managers and general users shall report any policy breach they become aware of to the Office Manager.

3.0 PURCHASE OF HARDWARE AND SOFTWARE

Hardware and software shall not be purchased by individual users or divisional groups. All hardware and software requirements shall be communicated to the Office Manager with an explanation of why the hardware or software is required and the business benefits that will be provided by the purchase. The Office Manager shall arrange approval and be responsible for all purchases in accordance with the current Statement of Commercial Responsibility Levels.

4.0 SOFTWARE

4.1 General Requirements

Software shall be installed (or arranged to be installed) by the Office Manager only. This includes applications, utilities, demonstration software, business applications, operating systems and operating system upgrades and program patches and upgrades.

Under no circumstances shall pirated software be loaded onto any Bardavcol's computing hardware. Unauthorised software is defined as any software and/or data to which Bardavcol have no legal right to use. Unauthorised software is also defined as using software on more stations than Bardavcol's licensing agreements permit and also includes free ware and share ware.

Software piracy is a serious crime. A semi-government body now exists to enforce the laws on this issue, having the power to raid companies and seize all computers. Penalties are harsh and companies can be fined considerable amounts. Individuals can also be held liable with gaol terms enforceable.

Games and other entertainment software shall not be permitted on Bardavcol's computers, either during or out of working hours

Software configurations shall not be changed by users. All configuration changes shall be performed in consultation with the Office Manager. This includes start-up files, Windows files, application settings and network settings.

Please be aware that the Office Manager shall regularly audit PCs to ensure compliance with this policy. Any unauthorised software located on machines shall be deleted and disciplinary action may be taken.

4.2 Virus Protection

The most common way a virus is introduced to a computer system is via a file loaded, accessed or executed from an external source, such as a , usb attached device. email or the Internet.

To ensure that Bardavcol is protected against computer viruses, virus detection software shall be installed on all computers. If a computer does not have this software installed the user shall contact the Office Manager immediately. When connected to the Head Office network virus software shall be automatically updated by the server.

The virus detection software used by Bardavcol has been configured to automatically scan drives and CD ROM media. This function should not be disabled by the users. Therefore, any software brought into Bardavcol, such as CD Roms and USB’s obtained from external parties, shall be scanned for viruses prior to being downloaded.

If users suspect, or if the virus software detects a virus, the Office Manager should be contacted immediately. The personal computer should not be used in any way until the Office Manager has resolved the problem.

5.0 HARDWARE

Reasonable steps shall be taken to protect hardware from loss or damage.

Laptop/notebook computers shall be secured when left on business premises overnight and locking them in cupboards or filing cabinets and removing the keys.

Users who choose to take their computers home or offsite require authorisation to do so by the Office Manager. Users are responsible for any computer that is issued to them and steps shall be taken to ensure its security at all times, for example, computers shall not be left unattended in motor vehicles.

If a user’s computer is stolen or damaged and the company management considers that the actions of the user contributed to the theft or damage the user may be responsible for its replacement or repair.

Please be aware that the Office Manager shall regularly audit company hardware to ensure compliance with this policy.

Hardware and peripherals shall not be moved between divisional groups without the prior consent of the Office Manager.

Under no circumstance should hardware be repaired, or covers removed by users. Hardware problems shall be reported to the Office Manager who will resolve the problem personally or organise repairs to be performed. Users shall not contact hardware suppliers directly but shall liase with the Office Manager.

Any hardware that is due to be made redundant shall have their hard drives completely and securely erased by the Office Manager.

Any personal hardware that shall be connected in conjunction with any Bardavcol hardware must be authorised by the Office Manager (eg personal organisers, mobile phones etc.)

Any hardware required to be added to the network must be first authorised by Office Manager (e.g Ethernet, modem cards).

6.0 SECURITY

6.1 Passwords

Password security is an accepted first line of defence against unauthorised use of a user's computer.

An IT security violation can occur when an authorised user deliberately accesses, or attempts to access, computer equipment for personal benefit or gain, to destroy data in order to disrupt business or for any other reason.

Drives that are shown under a users own username and password are the only drives that users have permission to access.

Examples of security violations include:

- Attempting to access a computer system or function within a system without authority;
- Attempting to log on with someone else's User ID;
- Accessing and supplying data to an unauthorised user;
- Installing unauthorised software or hardware on Bardavcol IT equipment;
- Removing IT equipment from Bardavcols premises without proper authorisation;
- Providing your password to another individual so they can gain unauthorised access: or
- Falsifying or updating records and systems without proper authorisation.

If a user believes that another individual has become aware of their password, they should change their password immediately and/or contact the Office Manager for assistance.

Any computer that is used in a location other than Head Office (Dry Creek) shall have password protection activated and shall also make use of screen saver password protection. These passwords shall be set to the company standard as advised by the Office Manager.

Complex Passwords are required and must meet the following minimum requirements:-

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least eight characters in length
- Contain characters from three of the following four categories:

  English uppercase characters (A through Z)

  English lowercase characters (a through z)

  Base 10 digits (0 through 9)

  Non-alphabetic characters (for example, !, $, #, %)

- Do not use a sequence of keyboard characters (eg. 123456);
- Do not use words which may be easily guessed (eg. user's name);
- Users will be required to change their passwords every 90 days

It is the user's responsibility to ensure that they choose a password that will not be easily guessed

6.2 *Data Security*

The following network drives shall be used for data storage purposes:

- The J:\ drive (common) is accessible for all PC Users, but shall *not* be used to store any unauthorised data. This drive is used for shared files which need to be accessed by more than one group of users.
- NOTE: All data stored on this drive is accessible and can be modified by *any* user.. All sensitive, valuable, or critical information held on computers shall be backed up.
- User's shall make a duplicate copy of files not stored on a backed up network drive by copying those files to external storage (for non-networked PCs).

Loss of data must be notified to the Office Manager as soon as possible to ensure full recovery (for data that has been backed up on the network). Users are to notify the Office Manager immediately to ensure swift recovery of data. The longer it takes to find out about the data loss, the less likely it is that the data can be recovered.

Users shall save files frequently (eg. every five minutes) to protect against loss due to PC or network failure.

7.0 ELECTRONIC MAIL

Electronic mail (e-mail) provides Bardavcol with a rapid, easily used, and written communication medium. All messages generated on, or handled by this facility, including backup copies, are the property of Bardavcol, and not the property of users.

Electronic messages are formal business communication and have the same legal status as letters, memos and other printed communication. Both hard copies and electronically stored copies of e-mail communications are subject to the laws of defamation, harassment, copyright and/or privacy.

E-mail is not a secure medium. Messages are routed using the Internet and can be forwarded, intercepted, printed, and stored by others. Bardavcol currently do not utilise data encryption and messages shall never contain sensitive company information.

Users are expected to maintain the highest standard of business etiquette when preparing e-mail messages and shall never include remarks or comments about staff, projects or other companies that are, or could be interpreted as, slanderous or disparaging.

Any e-mail correspondence, either inward or outward, shall be treated in the same manner as all Bardavcol correspondence, particularly with regard to circulation and filing.

An e-mail message is like any other written communication, particularly when sent to an outside organisation, it represents Bardavcol.

Job numbers/tender reference and project description shall be shown on all outgoing e-mail correspondence. Ensure messages do not contain spelling errors and that they are grammatically correct.

E-mail messages shall contain a disclaimer in the following format:

> *"The information in this e-mail is confidential, it is intended solely for the addressee. Access to this e-mail by anyone else is unauthorised. If you are not the intended recipient, any disclosure, copying, distribution or any action taken or omitted to be taken in reliance on it, is prohibited and may be unlawful."*

The following activities shall be prohibited when using e-mail facilities:

- Forwarding chain e-mails;
- Using or copying software in violation of license agreements of copyright;
- Forwarding intellectual property without the consent of the original sender;
- Excessive usage of the e-mail facility for personal communications.

8.0 INTERNET USAGE

Bardavcol will invoke the right to monitor or audit staff compliance with this Policy relating to usage of Internet facilities.

Detailed logs of every employee's web browsing and internet activities can be stored by Bardavcol and the Office Manager shall have the right to access these logs if staff compliance becomes an issue of concern.

The Office Manager shall be responsible for installing and configuring Internet access software. Users shall not alter software configuration or install additional or alternate Internet software.

Bardavcol's primary use of the Internet shall be to provide cost effective, efficient communication. Internet access for the purpose of 'surfing' is restricted to legitimate and justifiable company business both during work hours and after hours.

The following activities shall be prohibited when using the Internet:

- Unless downloaded information is for business purposes it shall not be downloaded or installed on any Bardavcol PC or laptop.
- Intentional sending, downloading, displaying, printing or otherwise disseminating material that is sexually explicit, obscene, profane, harassing, discriminating, fraudulent, offensive, defamatory or otherwise unlawful;
- The playing of games;
- Viewing any video site material except for valid business purposes
- Using or copying software in violation of license agreements or copyright;
- Violating State, Federal or International law;
- Use of the Internet for personal business or private purposes;
- Engaging in online chat groups or real-time exchange.
- Browsing of any social media (facebook, instagram, twitter etc)
- No online purchasing unless for the purposes of the company

All files downloaded from the Internet and file attachments received via electronic mail shall be screened with virus detection software.

Technical and/or business information taken off the Internet shall be considered suspect until confirmed by separate information from another source. There is no quality control process on the Internet and a considerable amount of information is outdated or inaccurate.

9.0 VIRTUAL PRIVATE NETWORK

Approved users and authorised third parties (clients, subcontractors, consultants etc) may utilise the benefits of VPN's to access Bardavcol resources.

Additionally:

- It shall be the responsibility of employees with VPN privileges to ensure that unauthorised users are not allowed access to Bardavcol's internal networks.
- VPN use to be controlled using either a one-time password authentication such as a token device or a public/private key system with a secure pass phrase.
- When actively connected to the corporate network, VPN's will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
- Dual (split) tunnelling shall not be permitted; only one network connection is allowed.
- VPN gateways will be set up and managed by Bardavcol networks operational groups.
- All computers connected to Bardavcol internal network's via VPN or any other technology must use the most up-to-date virus software that is the corporate standard; this includes personal computers.
- VPN users shall be automatically disconnected from Bardavcol's network after thirty minutes of inactivity. The user must then login again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
- Users of computers that are not Bardavcol owned equipment must configure the equipment to comply with Bardavcol VPN and network policies. The Office Manager will provide standard configuration protocol.
- All VPN traffic must be encrypted;
- VPN users shall not disclose any connection details to unauthorised personnel;
- By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Bardavcol's network, and as such are subject to the same rules and regulations that apply to Bardavcol owned equipment, ie their machines must be configured to comply with Bardavcol's Security Policies;

10.0 REMOTE ACCESS

Remote access to the Bardavcol network resources is via Remote Access (RDP) to the internal Remote Desktop servers (Terminal Servers).

The access is via a Remote Desktop Gateway to ensure encryption and security of company data.

- Access to Remote access will need to be granted by the appropriate Manager
- It shall be the responsibility of users with Remote Access privileges to ensure that unauthorised users are *not* allowed access to Bardavcol’s internal networks.
- All Remote Access users will need to have a valid password which meets or exceeds the password complexity requirements.
- When Remote Access is used from a remote site the user shall *not* leave the computer unattended whilst it is signed into the network.
- All computers connected to Bardavcol internal network’s via Remote Access or any other technology must use the most up-to-date virus software that is the corporate standard; this includes personal computers.
- By using Remote Access with personal equipment, users must understand that their machines are a de facto extension of Bardavcol’s network, and as such are subject to the same rules and regulations that apply to Bardavcol owned equipment, ie their machines must be configured to comply with Bardavcol’s Security Policies.

11.0 SMART PHONES, TABLETS AND MOBILE DEVICES

Mobile devices including smart phones and tablets now have the ability to access the internet, email and have remote access to Bardavcol’s resources via VPN or Remote Access.

In addition to complying with the policies described herein, due to the portable nature of these devices, extra precautions need to be taken.

Once configured, a mobile device does not usually require a further password to access Bardavcol email or Remote Access to Bardavcol.

This makes the Bardavcol data particularly vulnerable in the case of loss, theft or use by an unauthorised person.

To ensure the security and integrity of the company data, the following steps need to be taken:-

- No mobile device is to be configured to access Bardavcol Email or Bardavcol Remote Access servers without prior permission of the appropriate manager
- All mobile devices are to be secured with an appropriate password (4 digit PIN is not sufficient)
- All mobile devices (as far as technically possible) are to have mobile tracking enabled to allow the phone to be remotely wiped if lost or stolen

- Each user is to ensure that the mobile device is not used by other persons (eg members of the family). This could put Bardavcol data at risk
- The mobile device will be a de-facto extension of Bardavcol's network, and as such is subject to the same rules and regulations that apply to Bardavcol owned equipment, ie particularly in relation to Security and Internet Usage.
- Bardavcol has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.
- While IT will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- The company reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

12.0 NON COMPLIANCE

Any case of non-compliance by users must be reported to the Office Manager and the users Applicable Manager in order to rectify the breach in the Computer Security Policy and to decide which course of action is required.