INFORMATION SECURITY POLICY

1. Intent and Scope

This cybersecurity policy(policy) provides the basis of cybersecurity management within Because Brand Experience PTY LTD (trading as Because Creative Experiences).

This policy applies to all of Because Brand Experience PTY LTD employees, contractors, volunteers, vendors and anyone else who may have any type of access to Because Brand Experience PTY LTD systems, software and hardware.

Effective protection of business information creates a competitive advantage, both in the ability to preserve the reputation of Because Brand Experience PTY LTD and in reducing the risk of the occurrence of negative events and incidents.

2. Password Requirements

To avoid employees' work account passwords being compromised, these best practices are advised for setting up passwords:

(a) Use at least 8 characters (must contain capital and lower-case letters, numbers and symbols)

(b) Do not write down password and leave it unprotected

(c) Do not exchange credentials when not requested or approved by supervisor

(d) Change passwords every 1 months

3. Email Security

Emails can contain malicious content and malware. In order to reduce harm, employees should employ the following strategies:

(a) Do not open attachments or click any links where content is not well explained

(b) Check the email addresses and names of senders.

(c) Search for inconsistencies

(d) Block junk, spam and scam emails

(e) Avoid emails that contain common scam subject lines such as prizes, products and money transfers

If an employee is not sure that an email, or any type of data is safe, the employee should contact Meredith Cranmer.

4. Device Security and Using Personal Devices

Logging in to any work accounts for personal devices such as mobile phones, tablets or laptops, can put Because Brand Experience PTY LTD data at risk. Because Brand Experience PTY LTD does not recommend accessing any Because Brand Experience PTY LTD data from personal devices. However, if this cannot be avoided, employees are obligated to keep their devices in a safe place and not exposed to anyone else.

Employees are recommended to follow these best practice steps:

(a) Keep all electronic devices' passwords secure and protected

(b) Logging into accounts should only be performed through safe networks

(c) Install security updates on a regular basis

(d) Upgrade antivirus software on a regular basis

(e) Never leave devices unprotected and exposed

(f) Lock computers when leaving the desk

5. Transferring Data

Data transfer is a common cause of cybercrime. Employees should follow these best practices when transferring data:

(a) Avoid transferring personal information such as customer data and employee information

(b) Adhere to the relevant personal information legislation

(c) Data should only be shared over authorised networks

(d) If applicable, destroy any sensitive data when it is no longer needed

6. Physical Documents

Employees are required to ensure that:

(a) All sensitive and confidential information in hardcopy form is secure in their work area at the end of the day (b) Printed documents containing sensitive and confidential information should be immediately removed from the printer

(c) Any sensitive and confidential information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day

(d) File cabinets containing sensitive and confidential information must be kept closed and locked when not in use or when not attended

(e) Keys used for access to sensitive and confidential information must not be left at an unattended desk

(f) Upon disposal of sensitive and confidential documents, documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins

(g) Whiteboards containing sensitive and confidential information should be erased

7. Working Remotely

When working remotely, all cybersecurity policies and procedures must be followed.

8. Acceptable Use

User accounts on work systems are only to be used for the business purposes of Because Brand Experience PTY LTD and not to be used for personal activities.

Employees are responsible for protecting all confidential information used and/or stored on their accounts. This includes their user logins and passwords. Employees are prohibited from making unauthorised copies of such confidential information and/or distributing it to unauthorised persons outside of Because Brand Experience PTY LTD.

Employees must not purposely engage in any activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to Because Brand Experience PTY LTD systems for which they do not have authorisation.

9. Security Requirements

Employees must not install unauthorised software.

Employees must not use unauthorised devices on their workstations, unless they have received specific authorisation from Meredith Cranmer.

Employees must not attempt to turn off or circumvent any security measures.

Employees must report any security breaches, suspicious activities or issues that may cause a cyber security breach to Meredith Cranmer.

10. Disciplinary Action

If this policy is breached, one or more of the following disciplinary actions will take place:

(a) Incidents will be assessed on a case-by-case basis

(b) In case of breaches that are intentional or repeated or cases that cause direct harm to Because Brand Experience PTY LTD employees may face serious disciplinary action

(c) Subject to the gravity of the breach, formal warnings may be issued to the offending employee

11. Data Storage and Retention

(a) **How the Data is Stored:** All sensitive data collected by Because Brand Experience PTY LTD is securely stored on Microsoft sharepoint and backed up securely by R2 networks. Physical and digital access controls are in place to prevent unauthorised access to sensitive information.

Each of the third-party platforms we use stores customer data on their secure servers. Data is stored per each platform's privacy policy and complies with standard data protection protocols.

1. Survey Monkey
2. Mailchimp
3. Obee

(b) **Where the Data is Stored:** All data is stored on Sharepoint and we have appropriate processes and controls in place to prevent data loss / manage security. Local backups are also maintained in a secure off-site facility to ensure data redundancy.

(c) **How Long the Data is Stored:** Data is retained for as long as it is needed for business or legal purposes. In general, data is stored for a period of 3 months, after which it will be securely disposed of unless a longer retention period is required by law or business needs. Data can be deleted within each platform according to each client's data retention requirements. We can manually set retention periods or delete records upon request, ensuring data is disposed of securely and responsibly in line with our client's cybersecurity policies.

(d) **Softwares Used to Capture Data:** For data collection during activations, we work primarily with Survey Monkey, Mailchimp, and Obee depending on the type of activation. These platforms handle customer sign-ups, bookings, and survey data. Customers may enter data on a website operated by Red Crystal Agency, but no customer data is stored on these systems.

NEXT REVIEW: JANUARY 2026