Chill Out!
event management

Security Policy

Version 1.03, 04/09/2020

Contents

Introduction/purpose .... page 2

Roles & responsibilities .... page 2

Acceptable use policy .... page 3

Authentication & network access policy .... page 8

Network security policy .... page 8

Back up policy .... page 8

Password policy .... page 8

Confidential data policy .... page 9

Incident response policy/Data breach .... page 10

Employee departure policy .... page 10

Control and Maintenance of the Policy .... page 11

Introduction/purpose

This Security Policy sets out specific areas where Chill Out Event Management (The Company) has identified potential risks to security. Notwithstanding the contents of this policy all employees should be security aware at all times both on and off premises and should use common sense to protect the company, its employees and its customers at all times.

The security of Chill Out Event Management systems, assets, data, employees and customers is of the utmost importance to the success and future of the company especially in an environment of increasing threats from fraud, and criminal acts linked to IT and internet services.

The purpose of this document is to ensure that Chill Out Event Management has adequate security mechanisms and procedures in place to protect the company, its assets, employees and customers from malicious or accidental lapses, leaks or theft of data that the company is legitimately required to hold in the normal conduct of its business.

This policy should be read in conjunction with the company's Privacy policy.

Failure to comply with this policy or the company Privacy Policy could constitute a serious disciplinary matter which could result in dismissal for gross misconduct.

Roles & responsibilities

It is the duty of the General Manager to ensure:

- All requirements described in this document are available to, understood and enforced by all employees.
- That newly recruited employees are aware of the policy and its requirements and receive the appropriate training
- That the policy relating to employee departure is applied appropriately to each specific case.

It is the duty of the General Manager to ensure:

- That adequate and appropriate technology is in place to protect the company's assets from theft or malicious access
- That client data and the company's intellectual property is adequately stored and protected from unauthorised access or modification
- In their role of Data Controller, that the company's Privacy Policy is current and adequate to protect the company's and clients Personal Data as defined by the policy
- That the premises has adequate security mechanisms in place when unattended

It is the duty of the IT Systems Administrator: Contracted to Jose Dias, Sublatum to ensure:

- All backups are successful
- All software patches and updates are in place
- All employees have the correct permissions to access the data they need to fulfill their responsibilities

- Employees can only access data that is required for them to carry out their job
- The employee departure policy is followed per the instructions issued by the General Manager

It is the duty of every employee of Chill Out Event Management to:

- Understand and apply the Company's Security Policy and Privacy Policy
- Report any possible or suspected data or other security leakages to Management

Acceptable use policy (internet, email & social media)

All employees must follow the acceptable use policy at all times when accessing the company's computer network or using any web based services i.e. browsing the Internet or using email regardless of the method. Employees are also responsible for ensuring that any guests accessing the web via the Company's internet connection are aware of and adhere to this policy.

If given any passwords or login details to access the computer networks, systems or services, all employees of the company accept and agree to be bound by the Company's acceptable use policy.

Information Systems, including Social Media networks

Chill Out Event Management provides a variety of computer hardware systems, software applications and Internet access for all users, so that they may communicate efficiently, access information sources and databases and execute all tasks relevant to the business and in order to accomplish company business goals.

Viruses and similar problems can bring an entire computer network to a standstill. It is important, therefore, that all employees are aware of the need to act responsibly and minimise the risk of this occurring. To help protect the company network, employees must not download any documents on to a computer belonging to the company without being confident that it comes from a legitimate source. If in doubt, request assistance from the Operations Director or IT Systems Administrator.

Chill Out Event Management computer equipment and any software tools must be used for professional purposes only and any use is subject to the following general conditions:

- Passwords and any specific company computer equipment provided to you must be used by you only and exclusively in the performance of your job responsibilities. All passwords and login details must be treated as confidential information and must not be disclosed under any circumstances to third parties.

- The Company specifically prohibits employees using company computer systems or on-line access for any illegal purpose, whether in the course of business or otherwise, for example (but without limitation):

- Gaining unauthorised access to or intentionally damaging other computer systems or networks or the information contained within them.

- Distributing or obtaining illegally copied software, data, graphics, sounds, text or other material.
- Sending or posting harassing or threatening messages or pornographic or patently indecent content via any means including via personal Social Networking sites.
- Committing theft, fraud or other criminal acts of any kind.

Chill Out Event Management will co-operate fully with law enforcement authorities to prosecute offenders.

You must report any suspected, accidental, or intentional illegal action to the Operations Director

The company has the right to monitor all on-line communications to ensure that appropriate business and lawful purposes are being pursued and to limit connections solely to business-related resources.

All information stored on the company IT systems belong to Chill Out Event Management. The Company may inspect all such computer systems and information at any time as necessary for the conduct of its business.

No direct third party physical or electronic access to company facilities, information or computer systems of any type or for any reason may be established without the express permission of the Company (this includes use of the company's Wi-Fi network for personal technology).

Theft of Company trade secrets or Company confidential proprietary information contained in any media (electronic or other), including unauthorised disclosure of Company data or databases to third parties or unauthorised use thereof for personal benefit or the benefit of third parties, is strictly prohibited.

Electronic Mail

The company provides localised and web-based email facilities, including identity email accounts and aliases to all employees for purposes of business communications. Occasionally these facilities may be extended to business associates.

You are prohibited at all times, when using any of the message services available to you, from initiating or forwarding harassing, pornographic, indecent or discriminating messages, either to other members of the company or to anyone else.

Electronic mail must be addressed to proper recipients. Carefully check to reduce the possibility of communications being misdirected. If your job includes responding to work-related email requests on an informal and unofficial basis, make sure that your message clearly states that your views are not necessarily the views of the Company. Even so, you must be aware that the address you are sending from may well indicate the Company's name and you should keep in mind that the message may be seen to be representing the Company, regardless of any disclaimers. Therefore, do not send any email directly critical of the Company's vendors, clients, employees or services. Do not say or do anything else that you wouldn’t say or do in front of a client, and in all cases, do not reveal any confidential information of the Company or its vendors, clients and employees.

You are prohibited from misrepresenting your name, identity or position or posing as another person in an electronic mail message to any recipient.

Email should never be used as a medium of exchange for confidential information due to its vulnerability to interception. It is strictly forbidden to send any information which may amount to a trade secret or confidential information belonging to the Company or any of its clients over the Internet unless suitable encryption is used.

Always make hard copies of email messages which are important or which you may need to retain for legal or general record keeping purposes. In particular, if you send an email, with or without an attachment, to a client keep a copy in the client’s file in the same way that you would retain a copy of any other document.

Always request verbal or written confirmation of receipt of important email messages. Do not just rely on an automated notification of receipt.

Ensure that you do not enter into contractual commitments by email without the proper authorisation. Emails, like letters, internet postings, faxes and telephone calls, can create binding contracts. Beware of agreeing to commitments unintentionally. Always seek the correct authorisation from the General Manager or a Director of the company.

Do not download copy or transmit to third parties the works of others without the express permission of the person who wrote the work. Not only is this a breach of confidence but it may also infringe copyright. Always keep a record of permission given to copy work to a third party.

While reasonable levels of personal email is acceptable, excessive use of email for personal purposes may result in disciplinary action. A log of all mail traffic is kept and analysed on a regular basis.

Checking your email from a remote location: Email is accessible via the Company Webmail from any internet-enabled computer by typing the following web address webmail.chill-out.co.uk using a safe modern browser; (If you experience difficulties logging on to Webmail please contact the IT Systems Administrator.

E-Mail Out of Office Setting: If you are going to be out of the office for a prolonged period you must enable your Out of Office settings to notify people that you will be out and when you will be returning. A standard message will then be sent to anyone that emails you whilst out of the office.

Adopt good housekeeping habits.

Do not send trivial emails. They block up the system.

Always delete messages which are no longer needed. The IT Systems Administrator will regularly check that housekeeping is done and will ask you to delete old messages where appropriate.

Remember to save or print off all those important documents which you may need to keep before deleting them in email.

Beware that it is possible to retrieve deleted messages from your computer. It is important to remember that emails are disclosable in court proceedings if they are relevant. Therefore any employee who becomes involved in potentially litigious matters on behalf of the Company should refrain from communicating to anyone about those matters via email.

Do not use emails for personal advertisements.

Never rely solely on emails for business critical messages. There is no guarantee that the email will be received by the intended person at all. Always confirm by telephone that the message has been received and understood.

The World Wide Web

The Company provides Internet access to assist employees in their job responsibilities.

Whilst using the Company's IT infrastructure or your own personal IT system the following rules apply:

Use of the Internet for Chill Out Event Management work is intended for business purposes only.

You must verify that any information obtained from the Web is from a reliable source prior to using the information for business related purposes. Preference should be given to official sites (or their authorised mirrors).

There is a wide variety of content available on the Web other than that which you use for work. Keep in mind that Web usage is intended to be exclusively for the Company's purposes and any content transmitted by you on the World Wide Web, for example on personal web email sites or social networking sites, whether during or out of office hours which relates to the company or any employee of the company can be used as evidence against you in a disciplinary situation and result in dismissal in cases of gross misconduct.

Downloads of software applications or executable files from the internet must be authorised prior to download by contacting the IT Systems Administrator.

You are not permitted to download executable files to install online games or unauthorised software applications on the network or your computer.

The Company specifically prohibits the use of the Web or any other electronic communications services or equipment to access or transmit pornography and or indecent materials. The Company retains sole discretion to determine what constitutes such materials.

These rules also apply for proprietary on-line services, searches or subscription services, and similar information access methods.

Computer Software and Databases

All company owned software is only for use on Company computer systems and strictly in accordance with the license agreement. Unless otherwise provided in the license, any duplication of copyrighted software, except for backup and archival purposes, is a violation of the law.

No employee shall destroy or modify Company software or implement bugs, viruses, trapdoors, time bombs or other disabling devices or any other code which would have an adverse effect.

Company databases are valuable sources of intellectual property and contain confidential and proprietary information belonging to the Company. They may only be accessed through the Company's computer systems for business purposes. No employee shall destroy or modify company databases or implement inaccurate data.

Disclosure to or use for the benefit of third parties is strictly prohibited.

Any employee who determines that there may be a purposeful or accidental violation of the above software policy within the Company shall notify the General Manager or Operations Director immediately.

If you think you have accidentally loaded a virus on to a company computer, switch off the machine/equipment immediately and contact the IT Systems Administrator urgently. Failure to do so could be construed as a disciplinary offence.

WARNING: COMPUTER CRIME

Anyone suspected of committing computer crime, whether under the Computer Misuse Act 1990 or otherwise, may by suspended with pay while an investigation is carried out and, depending on the outcome of the investigation, dismissed for gross misconduct.

Examples of criminal offences include any attempt to gain unauthorised access to programs or data held on a computer and subjecting the contents of a computer system to an unauthorised modification.

Passwords

Access to the organisation's computers is password protected. Employees are required to use their passwords, and not put in place any process which bypasses the requirement for a password. Passwords must not be stored by the computer.

Passwords must not be disclosed to any other person.

If you believe your password is known by another party or you wish to change it, please contact The IT Systems Administrator urgently.

Software or Hardware Issues

For assistance with any software or hardware malfunction, please contact the IT Systems Administrator immediately with a CC of the email to the General Manager and Operations Director.

Authentication & network access policy

The company's computer systems have 3 levels of password:

1. All company computers i.e. laptops and pc's have full disk encryption requiring the user to provide a unique log on. The unique log on is only known to the user and the IT Systems Administrator. The system will lock out after 5 failed attempts.
2. Second level unique password known only to the user and the IT Systems Administrator is required to give the user access to the computer software and network . This second level of password is covered by standard windows security recommendations for password syntax.
   a. This second password level also defines access to specific network resources unique to each user.
3. There is third level password security for email access unique to each user/email account.

All network resources are only accessible via VPN (Virtual Private Netword) which is secured by shared private keys.

Network security policy

While off premises each company owned machine is secured by a private secure asymmetric firewall.

In addition, whilst in the office the office network and telecoms systems are protected behind a primary firewall which is provided by an offsite third-party.

The office network includes a secondary encrypted email backup server. The primary servers are held offsite in a secure private cloud facility.

VPN access is only available via secure company equipment

Back up policy

The company operates 3 levels of backup:

1. Nightly backup on a private cloud. This is stored on a redundant encrypted server in a secondary location. In addition, the company runs a nightly version backup.
2. Realtime full email encrypted back-ups which includes entry and exit from the server. Provided by a third-party.
3. In addition, we run a secondary encrypted email back-up to a local server in the office.

Password policy

1. Disk encryption password are changed annually or sooner if required.
2. User profile passwords are issued by the IT Systems Administrator and changed periodically. The passwords follow standard accepted security syntax.
3. Email passwords are randomized 12-digit codes provided by the IT Systems Administrator. The passwords follow standard accepted security syntax.

4. Document passwords are assigned in line with the event code
5. The guest Wi-Fi network has an assigned password set by IT Systems Administrator. This password only provides internet access.
6. The company private Wi-Fi network has an assigned password set by IT Systems Administrator. This provides full network access subject to the normal computer system passwords.

Confidential data policy

Secure company data is categorized in two levels: 1. Restricted Data 2. Confidential Data. Definitions of the types of data, details on access/movement and deletion rules are as follows.

In all cases when the company is acting as the data controller as defined under GDPR in the company Privacy Policy, Personal Data shall be deemed as Confidential Data unless specified otherwise in this policy.

***Restricted Data* –** Any data relating to the activities of or belonging to a Client (Excluding Personal Data)
***Access/movement* -** Restricted data may only be used or shared by and between the company's employees however it may also be shared with external third-parties when deemed essential and expressly for business purposes.

Confidential Data

- All personal data covered under the company Privacy Policy
- Company data falling into the following categories
  - Employee records
  - Financial data
  - Company facilities and information systems infrastructure
  - Any other data the company may deem to be confidential

Access/movement

- Confidential personal data is covered under the Privacy Policy
- Confidential company data may only be accessed by Senior Management and is to be stored only of the Management Drive. Hard copy data is to be stored in the company safe. Movement of confidential data is under the strict control of Senior Management.
- Employee records relating to payment of salaries and all financial data is also accessible by the finance manager and is stored on the 'Q' drive.

Deletion

- **Personal data**
  Deleted a maximum of 2 months after the need to use the data as detailed in the company Privacy Policy
- **Confidential data**
  Relating to personnel records is deleted 5 years after individual left the company. Other confidential data has no time limit for deletion and is retained on an as needed basis for business purposes

Notwithstanding the above, where longer periods are required for legal or government approved purposes confidential data may be retained for longer periods.

- **Restricted data**
  No time limit for deletion and is retained on an as needed basis for business purposes

Definition of Deletion:
All electronic, hardcopy or other information however stored shall be deleted as follows:

- **Removal from live system:**
  Immediate as per the deletion schedule above.
- **Removal from the back up:**
  6 months after removal from live system.
- **Removal for GDPR purposes:**
  Right to Erase. Actioned on a case by case basis.

Incident response policy/Data breach

If you have reasonable grounds to suspect there has been a data breach, you are required to take the following steps:

1. Record the date and time of the breach
2. Alert the Data Controller/Operations Director and the IT Systems Administrator
3. Where possible stop any further data loss from the breach
4. Document the nature of and all the findings of the breach
5. Interview all the people who have been involved in the breach
6. Review all security procedures and controls
7. Recover infected machines (system recovery)
8. Notify law enforcement as appropriate
9. Data Controller/Operations Director to notify customers that their data might have been affected in the breach

Employee departure policy

Email and network access

Senior Management to notify IT System Administrator in writing that an employee will be leaving the company.

IT System Administrator will change the passwords as defined in the Authentication and Network Access policy.

Out of office auto response is set up on departing employee's account directing them to an alternative address for 30 days. Email is also auto forwarded to named employee.

After 30 days the email will continue to be diverted and the email account deleted.

If needed Senior Management can have access to the email account.

Equipment

All IT and other equipment issued to an employee is handed back to the company no later than the day of departure of the employee.

Laptops returned must include power supplies(s) when handed back.
IT Systems Administrator runs back up on the laptop of any remaining files if appropriate then undertakes a full reset of the hardware.

Control and Maintenance of the Policy

This Policy and the company Privacy Policy are the to be maintained and updated as needed but in all cases shall be reviewed and approved by the Operations Director no later than one year after the last version update.