

BG8 Entertainment NV

User Management Policy

Disclaimer

This document is prepared specifically for the sole purpose of BG8 Entertainment NV ("BG8").

No part of this document may be reproduced, transmitted or in any other way distributed without the prior written permission from BG8 .

All technologies, designs, implementations, trade secrets and business models described herein are the intellectual property of BG8 and/or its partners and is provided for information purposes only.

This document is provided "as is" without any warranty concerning its accuracy or quality. In no event will BG8 be liable for direct or indirect damages resulting from incidental defects or inaccuracies in this document.

BG8 reserves the right to review and modify digital copies of this document at any time without prior notice.

Contents

Policy Overview	3
Enforcement	3
Objective.....	3
Purpose.....	3
Scope	3
Acceptable Email Use	4
E-mail Viruses and Attachments.....	5
Information Confidentiality	5
Intent to enforce and monitor.....	5
Retention and Purging	5
Junk mail	5
Very large files	6
Protection of your terminal	6
Mail Storms.....	6
Use of 3rd party Mail platforms	6
Personal Usage	6
Instant Messaging (IM)	7
IM Viruses and Attachments.....	7
Information security	8
Intent to enforce and monitor.....	8
Personal Usage	8
Password Management.....	8
Guidelines to good passwords.....	9
Password Policy	10
System Level Passwords	11
Employment Termination.....	11

Policy Overview

The purpose of the Policy is to protect BG8' information assets from all threats, whether internal or external, deliberate or accidental. By this, we mean protection of BG8 ' data, applications, networks, and computer systems from unauthorized access, alteration, or destruction

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Companies contracted to BG8 found to be violating this policy will be deemed to be in breach of contract.

Objective

This Policy has been developed to protect all systems and assets within BG8 to an adequate level from events which may jeopardise business activity. These events will include accidents as well as deliberate behaviour designed to cause disruption.

1. The primary objective of this policy is to ensure business continuity and minimise damage by preventing and minimising the impact of security incidents.
2. The secondary objective of the policy is to ensure BG8 ' compliance from a regulatory, contractual, and legal perspective.

Purpose

The purpose of security by way of user management and is to preserve an appropriate level of the following:

- Confidentiality: The prevention of the unauthorised disclosure of information
- Integrity: The prevention of the unauthorised amendment or deletion of information
- Availability: The prevention of the unauthorised withholding of information or resources

Scope

The Policy applies to all employees of BG8 . It also applies to contractors, consultants and visitors, not employed by BG8 but engaged to work with or who have access to company information, e.g. computer maintenance contractors.

Acceptable Email Use

BG8 provides employees with access to a variety of information technology systems and electronic communication media including Email and Instant Messaging for the pursuance of company business.

Users are responsible for drafting all emails carefully, avoiding any form of discrimination, harassment, and defamation, whilst taking into account any company representation and Data Protection issues.

Messages that are created, sent or received using the BG8's email system are the property of BG8, and as such BG8 reserves the right to access and disclose to relevant entities the contents of all messages created, sent or received using its email system.

- Emails are a form of corporate communication and therefore should be drafted with the same care as letters.
- Before sending proof read to make sure your message is understandable and appropriate.
- Do not send sensitive or emotional emails. If you are angry re-read it after you have calmed down.
- Never draft an email solely using CAPITALS – use normal sentence case.
- Employees must not play practical jokes, engage in pranks, or otherwise humorously make it look like a security incident is taking place, will take place, or has taken place when this is not true.
- Sexual, ethnic, and racial harassment, including unwanted telephone calls, electronic mail, and internal mail, is strictly prohibited. If such messages are received by employees, they must speak directly to the sender of offensive communications. If such offensive messages do not cease, they will be reported to their manager and the Human Resources department where disciplinary action will be taken.
- Before sending an e-mail, employees must verify that they are sending it to the correct contact. If it is suspected that an error has caused third party secret or confidential information to be exposed to unauthorised persons, these third parties must be immediately informed. If the third-party individuals are notified about breaches, or even seriously suspected breaches, they will be able to take protective action.

E-mail Viruses and Attachments

Employees are responsible for virus checking any attachment received before opening. Never open an attachment unless you are 100% certain of the sender AND have prior knowledge of the reason for the attachment being sent.

Information Confidentiality

Confidential and sensitive information is never to be sent unencrypted through end-user messaging technologies such as e-mail, instant messaging, or chat.

Email is an insecure method of communication with content easily copied, forwarded or archived. Sensitive information including but not limited to examples such as passwords or credit card primary account numbers (in clear text form), must never be sent by this means.

Obtain prior approval from your line manager before sending company information to external e-mail accounts (i.e. send a work document to your home email account, so to work on it further from home that evening). At no time should sensitive company information be sent, regardless of line manager approval.

Intent to enforce and monitor

BG8 reserves the right to carry out monitoring exercises on its systems, possibly without prior notice. Monitoring, via email blocking software may be used to block and read any email on BG8 ' network at any time by BG8 .

Retention and Purging

Deletion of old emails must be managed by each individual user, keeping in mind storage levels, archival levels, contractual evidence and legal discovery issues.

Junk mail

Email should not be sent to large numbers of people unless you are sure that it is directly relevant to their job. Sending unsolicited mail to many users ('spamming') is wasteful of user time and can disrupt the service, via performance delays, for other users.

Do not respond to or forward chain letters; or any other sort of spam using BG8 e-mail systems.

Very large files

Sending of large files should be avoided where possible. The use of appropriately licensed compression software (e.g. *.zip files) is advised.

Extremely large files should be sent by means other than email.

Protection of your terminal

Where terminals are left open and logged in when you leave your desk, a malicious user could send messages in your name. Ensure your terminal is locked or logged out.

Mail Storms

Avoid 'Mail Storms' – long discussions sent to a distribution list – consider verbal communication.

Use of 3rd party Mail platforms

Use of 3rd party e-mail systems such as "Gmail" or 'Hotmail' presents an uncontrolled channel for information flow both inbound and outbound. Such an uncontrolled channel may put BG8 in violation of its legal and contractual obligations and liable to prosecution, fine and or suspension of services.

Accordingly, the BG8 provides all users, whose job role dictates with access to BG8 sanctioned e-mail system. The use of any 3rd party e-mail systems is therefore strictly prohibited for business use.

Personal Usage

BG8 shall allow reasonable personal use of the e-mail system by its employee's. At all times all staff members, contractors and any other individual with access to BG8 ' e-mail system must abide by all the constraints and limitations set out within this Security Policy.

In addition, they must also abide by the following specific requirements:

- Do not use BG8 e-mail accounts for registration purposes in a public forum or similar context.
- Do not use it while posting messages in web forums or newsgroups, except when required to perform job function and approved by senior management.
- Do not use BG8 e-mail system for running your own business
- Do not send or illicit the receipt of excessive personal e-mails.

BG8 will make no differentiation between business and personal e-mails whilst conducting its previously stated monitoring activities.

Instant Messaging (IM)

BG8 recognises that IM is an invaluable resource and a key business tool and all communications on such media – including, but not limited to, Skype, WhatsApp, Telegram, WeChat, Messenger.

All communications on IM are to follow the same rules as e-mail in the section above. In addition, further care must be taken by users as IM is a real-time tool where conversations flow much faster than by email.

- Do not conduct sensitive or emotional conversations over IM. NEVER send company information via IM.
- If become angry during an IM conversation, do not engage in IM until after you have calmed down, consider drafting an e-mail or conducting a telephone conversation.
- Conversations of a more “formal” nature should not be held on IM. For example, this means dispute resolution, target/goal setting, conversations regarding fees, payments etc. These are more appropriate on email or telephone. If in doubt, do not use IM, use another forma

Users should be careful when accepting new contacts and sure ensure no new contacts are added without some form of prior arrangement.

IM Viruses and Attachments

IM represents a large risk to BG8 ; users are responsible and accountable for their actions whilst using IM and should adhere to the following guidelines at all times:

- Never send company information or files using IM.
- Never accept file transfers offered over IM.
- Never accept new 'Buddy' requests unless you are confident of the originator of the request.

Information security

IM is an insecure method of communication with content easily copied, forwarded or archived. Sensitive information including but not limited to examples such as passwords or credit card numbers, must never be sent by this means.

Intent to enforce and monitor

BG8 reserves the right to carry out monitoring exercises on its systems, possibly without prior notice. Monitoring, via IM blocking software may be used to block and read any IM on BG8 network at any time by BG8 .

Personal Usage

BG8 shall allow reasonable personal use of the Instant Messaging system by its employees. At all times all staff members, contractors and any other individual with access to BG8 ' Instant Messaging system must abide by all the constraints and limitations set out within this Security Policy.

BG8 will make no differentiation between business and personal messages whilst conducting its previously stated monitoring activities.

Password Management

Passwords are used for various purposes at BG8 . Some of the more common uses include user level accounts, web accounts, email accounts, screen saver protection, voice mail password, and local router logins.

Each member of BG8 should be assigned a system logon. Like your name, your logon is not secret, but your password is secret, it is very important that your password be protected.

Your logon and Password provide access to sensitive information and are used as authentication credentials for network access (e.g., VPN). The first task you perform is also one of the most important - choosing a good password.

The requirements for a strong password are:

- Minimum Length – 8 characters
- Maximum length – 14 characters
- Is NOT the same as your username
- Passwords should use three or four of the following four types of characters:
 - Lowercase
 - Uppercase
 - Numbers
 - Special characters such as !@#\$%^&*(){}[]

Guidelines to good passwords

Poor, weak passwords have the following characteristics:

- The password contains less than 8 characters.
- The password is a word found in a dictionary (English or foreign).
- The password is a common usage word such as:
 - Names of family, pets, friends, co-workers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software.
 - The words "Highland", "Hland", "H1ghland" or any other derivation.
 - Birthdays and other personal information such as address, car number plates and phone numbers.
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9,!@#\$%^&*()_+|~-
=\`{}[]:~<>?.,/)

- Are between eight and fifteen alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Use a phrase that has a number at the end of it
- Sometimes use capital letters, and sometimes use lower case letters. Use unusual capitalization in your phrase.
- Use a numerical representation of the letters of the alphabet for part of your phrase or one word in your phrase. For example, A is 1, B is 2, C is 3, etc.
- Use punctuation or special characters in part of your phrase.

Password Policy

Password Security

- Do not write your password down.
- Do not transmit your network password across the internet without it being encrypted.
- Do not use the same password on your computer at work that you may use to logon to a web site.
- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

Password Changes

Passwords must be changed every 90 days or at more frequent intervals. Whenever an employee suspects that a password has been compromised, that password must immediately be changed.

Password Storage

Passwords must not be stored in readable form; this means that passwords must not be written down or stored on a computer in some readily decipherable form. Should a password have to be stored, it should not be left in a place where unauthorised persons might discover it.

Sharing Passwords

Sharing of account login information is prohibited. The only time when a password should be known by another is when it is first issued. These temporary passwords must be changed the first time that the authorised user accesses the system.

Group Login

Each individual user needs to have a unique username and password; each member of staff should have a single unique user ID and a personal password for access BG8 ' computers and networks

Repeated Password Patterns

Users must not construct passwords with a basic sequence of characters that is then partially changed based on the date or some other predictable factor. Users must not construct passwords that are identical or substantially similar to passwords they have previously employed.

System Level Passwords

Passwords must be changed on a regular basis according to the following schedule:

- All system-level passwords (e.g., root, enable, admin, application administration accounts, etc.) must be changed every 30 days. All production system-level passwords must be part of the administered global password management database.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into e-mail messages or other forms of electronic communication.
- System-level passwords should never be authorised to subcontractors. Subcontractors must be logged in with system-level privileges by the Network Administrator.
- The Network Administrator must keep all system-level passwords in a sealed envelope with one of the members of the Executive Board.

Employment Termination

When a member of staff leaves the employment of BG8 , their user accounts are disabled as part of the leavers process.

Human Resources should inform any changes in worker duties or employment status promptly to the ISO and Key Official. For all terminations, the Human Resources department should also issue a notice of status change to all managers who might be responsible for a system on which the involved worker might have had access to. The terminated user's access rights should be immediately revoked.

Managers must ensure that staff leaving BG8 ' employment do not inappropriately wipe or delete information from hard disks. If the circumstances of leaving make this likely then access rights should be restricted to avoid damage to company information and equipment.

Prior to an employee leaving, or to a change of duties, line managers should ensure that:

1. The employee is informed in writing that he/she continues to be bound by their signed confidentiality agreement.
2. Accounts are disabled in order to deny access.
3. Relevant departments are informed of the termination or change, and, where appropriate, the name is removed from authority and access lists.
4. System administrative passwords known to the individual must be changed.
5. Reception staff and others responsible for controlling access to appropriate premises, are informed of the termination, and are instructed not to admit in future without a visitor pass.
6. Where appropriate, staff working out notice should be assigned to non-sensitive tasks or are appropriately monitored.
7. Departmental property is returned. Particular attention should be paid to the return of items which may allow future access. These includes personal identification devices, access cards, keys, passes, manuals & documents.

The timing of the above requirements will depend upon the reason for the termination, and the relationship with the employee. Where the termination is mutually amicable, the removal of such things as passwords and personal identification devices may be left to the last day of employment. Once an employee has left, it can be impossible to enforce security disciplines, even through legal process. Many cases of unauthorised access into systems and premises can be traced back to information given out by former employees.

System managers will delete or disable all identification codes and passwords relating to members of staff who leave the employment of BG8 on their last working day. Prior to leaving, the employee's manager should ensure that all PC files of continuing interest to the business are transferred to another user before the member of staff leaves. It is good practice for an 'exit' interview to be held during which the manager notes all the systems to which the member of staff had access and informs the relevant system managers of the leaving date. Special care needs to be taken when access to personally identifiable information, personnel information and commercially sensitive and financial information is involved.