

IT Acceptable Use Policy

<u>Document</u>	<u>IT Acceptable Use Policy</u>
<u>Version</u>	<u>1.5</u>
<u>Effective Date</u>	<u>14.10.2024</u>
<u>Domain</u>	<u>www.bombastic.com</u>

[IT Acceptable Use Policy](#)

[Document Information](#)

[Overview](#)

[Definitions of Terms Used](#)

[Scope](#)

[Introduction](#)

[General](#)

[Security](#)

[General Use and Ownership](#)

[Use of Resources](#)

[Employees and Interns](#)

[External Parties](#)

[Privacy](#)

[Security, Confidentiality and Intellectual Property](#)

[Online Activity](#)

[Social Media](#)

[Use of AI &/ AI tools](#)

Document Information

Overview

Definitions of Terms Used

The terms “must”, “will” and “shall” define a non-discretionary clause.

The terms “may”, “should” and “could” define a discretionary clause within certain business justified parameters.

The term “user” defines a person making use of company resources and may be used to refer both to employees/interns as well as consultants/contractors.

The term “company” will refer to the company that has assigned/is the owner of the resources assigned.

The term “resources” will refer to any system whether of a physical or digital nature. This applies to but is not limited to terms like hardware, software, services and data.

The terms “equipment”, “hardware” and “device” will refer to any physical device. This applies to desktops, laptops, phones and any other form of IT equipment.

The term “software” will refer to digital assets installed on an assigned device. This also includes cloud based software.

Scope

This policy applies to employees, interns, temporary workers, contractors, consultants and other workers working and/or providing services, including all personnel affiliated with third parties. This policy applies to all equipment owned or leased.

This policy also applies to the use of information, electronic and computer equipment and network resources to conduct business activities or interact with internal networks and business systems, whether owned or leased.

All employees, interns, temporary workers, contractors, consultants and other workers working for and/or providing services are responsible for exercising good judgement with respect to the appropriate use of information, devices, and network resources in accordance with policies and standards and laws and regulations.

This policy has been drafted in accordance with the applicable requirements of the Curaçao Gaming Authority and the relevant legislation of Curaçao.

Introduction

This section will provide a general overview of this policy in a point format. Each point provided here will be covered further on throughout the policy.

General

- Resources provided to users remain property of the company.
- The company retains full ownership and intellectual rights for output created on any company assigned resource.
- Users are not allowed to use personal devices to connect to company networks and/or to access company data unless explicit permission is granted by the CEO or IT Manager.
- Users are not allowed to make use of external storage devices.
- Users are not allowed to use corporate communication channels for personal use.
- Users are not allowed to transmit or receive any company data and/or undertake any communication via personal communication channels unless authorised by IT and the appropriate line manager. Should the requirement arise please contact IT for further assistance and approval.

Security

- The users shall at all times abide by the information security standards.
- The users shall take all precautions to ensure that resources entrusted to them by the company are protected to the best extent possible against misuse, loss, leaks and unauthorised access.
- The users must adhere in accordance to legal requirements, regulations, frameworks and standards such as but not limited to; GDPR, AML, PCI DSS.
- The users shall undertake any information security training deemed necessary by the company.
- Whenever possible the user shall avoid any form of shared authentication

General Use and Ownership

Use of Resources

Employees and Interns

- All employees and interns must carry their work only on company provided devices.
- Any form of data created and/or edited on any company provided devices remains the property of the company.
- Use of personal devices to access company resources and/or for work purposes is strictly forbidden unless authorised.
- Personal devices are only allowed to connect to any company network with prior authorisation and to be used only for recreational purposes only. This is covered in more detail in the BYOD (bring your own device) section in this document.
- All employees are responsible for exercising good judgement and follow best security practices including but not limited to; secure access of data, secure storage of data, encryption, password protection and multi-factor authentication whenever possible, general awareness of information security threats.
- All employees are expected to approach the Information Technology department in any case of doubt in terms of correct resource usage.

External Parties

- External parties such as but not limited to; contractors, consultants and suppliers are allowed by explicit CEO approval to use their own devices.
- Any work carried out for the company and/or on behalf of the company by external parties becomes the property of the company and the external party is forbidden from re-using, re-sharing or re-distributing this material with any other parties unless explicit consent is granted by the CEO.
- All external parties are responsible for exercising good judgement and follow best security practices including but not limited to; secure access of data, secure storage of data, encryption, password protection and multi-factor authentication whenever possible, general awareness of information security threats.
- External parties are forbidden from sharing any credentials provided to them even to colleagues within their own organisation.
- All external parties are expected to approach the Information Technology department in any case of doubt in terms of correct resource usage.

Privacy

While the company will strive to allow the user the best level of privacy, company owned and personal devices connected to the company network might be subject to inspection for security reasons.

Such inspection is of a security nature and is done only for threat prevention and data leakage prevention. Data inspection is done by the systems and is at no point accessible and/or viewable by any staff.

The exception to the above might occur only in exceptional circumstances where malicious intent is suspected such as but not limited to intentional data leakage and data theft.

Security, Confidentiality and Intellectual Property

- Any company information users access should be treated as confidential by default unless otherwise specified.
- Confidential information can be but is not limited to; corporate strategies, customer lists, supplier lists, research data and employee records.
- Intellectual property is any asset whether tangible or intangible created within and/or for the company. This can be but is not limited to; code, media, data, and training material.
- Credentials such as but not limited to; passwords, keys and tokens should be treated as confidential and highly sensitive, safely stored and never shared. If there is suspicion of any credentials being compromised, contact IT immediately.
- Portable devices such as but not limited to laptops and work phones are to be supervised by the respective assignee at all times.
- In the event any portable device is misplaced, lost or stolen this must be reported to the IT department immediately.
- The users are not allowed to disable, bypass or tamper with, even temporarily, any physical or digital security associated with company provided devices and/or services. Users are strictly prohibited from installing their own security software and/or attempting to add exceptions to the installed security software.
- The user is responsible for having the necessary precautions such as but not limited to anti-malware and firewall on any personal devices connected to the company BYOD networks.
- Personal devices which are non-compliant with the best security practices or deemed as a security risk will be blocked from all company owned networks without any prior notice and/or notification.
- Users shall lock their devices whenever they are not in front of them.

Online Activity

- Internet activity should be primarily for work purposes.
- Users are forbidden from accessing Internet resources of an offensive and/or explicit and/or illegal nature from company devices and/or from company networks. Such categories include but are not limited to; pornography/adult content, pirated content, racism, radical causes, illegal content, hacking, illegal drugs, phishing, fraud.
- Internet downloads should be limited to resources the users specifically need to carry out their roles.
- Users are not to disregard any warnings provided by the security solutions installed and enabled on their devices.
- Users are prohibited from accessing any form of dark web from company devices and/or from company networks.
- Users are forbidden from installing and using VPN and/or anonymisation software/services unless this is justified, approved and provided by the IT department.
- Any online software and/or service provided to the user is to be strictly used on the company provided devices and strictly for work purposes only.
- Users are to use the communication tools provided by the company such as but, not limited to email and chat, strictly for work purposes. Sharing of non-work related material on these channels is strictly forbidden.
- Users are expected to exercise good judgement and refrain from opening any suspicious material they might receive on any channel. In such cases IT should be consulted immediately for advice.

Social Media

Social media refers to the use of services such as but not limited to; Facebook, Instagram, Twitter, TikTok, Snapchat, LinkedIn and YouTube.

This section of the policy applies to all present and future services which fall under the social media classification.

- Users are forbidden from posting any company related material on any personal social media.
- Users are forbidden from sharing/posting any visual material related to the company and/or operation such as but not limited to; internal photos and/or videos of the office, photos and/or videos of company devices and photos and/or videos of persons within the office whether employees or visitors.
- Users are allowed to re-share official company announcements on social media provided that these originate from official company social media accounts.
- Users are allowed to use their personal social media accounts within reason and as long as these are not in violation of the above mentioned policies.
- Users with access to corporate social media accounts shall understand that these accounts are the property of the company and agree to have their details on record as having access to these accounts.
- Users with access to corporate social media accounts shall understand that posts on these channels should always adhere to the voice of the company and brands only. Posts on these accounts are not to reflect any personal/private thoughts and/or opinions.

Use of AI &/ AI tools

AI tools should only be used for assistance, suggestions, or enhancing productivity, not as definitive solutions or decision-makers.

Employees must not upload, input, or share any company-sensitive, confidential, or proprietary information into AI platforms, especially third-party tools that are not officially approved.

AI should complement human judgement, and all outputs must be reviewed for accuracy and appropriateness before use.

- Employees are prohibited from entering personal, customer, or employee data (including names, emails, financial records, or confidential business details) into AI tools that are not explicitly authorized by the company.
- The use of AI-generated notes or transcription services is only permitted within company-approved platforms such as Google tools. Third-party AI transcription services are not permitted due to security concerns.
- AI platforms should never be used to process, analyze, or store sensitive company documents or legal contracts.
- Employees must not upload images of individuals (including colleagues, customers, or third parties) into AI platforms, including for generating modified images, memes, or synthetic content, without explicit consent.
- Uploading or using AI-generated images that could misrepresent or manipulate someone's identity is strictly prohibited and may be a breach of GDPR and company policies.
- AI should not be used for facial recognition, biometric data processing, or any similar applications without prior legal and compliance approval.
- AI use must comply with GDPR, copyright laws, and other relevant data protection regulations.
- Employees must avoid using AI-generated content in ways that could mislead stakeholders or misrepresent factual information.
- AI-generated translations, summaries, or content should only be used as inspiration and not as final solutions towards the company brands.
- Employees are responsible for ensuring that AI-generated content does not contain biased, inappropriate, or harmful material.
- Any breach of this policy may result in disciplinary action, including loss of access to AI tools and other corrective measures as deemed necessary by the company.
- If you suspect an AI-related security or ethical issue, report it to the IT Security or Compliance team immediately.

This policy is subject to periodic review and updates to ensure alignment with evolving AI regulations and company security standards.