

SECURITY POLICY

Last updated: 24.07.2025

INTRODUCTION

The website betone.com is owned and operated by Continent Gaming N.V., a limited liability company registered in Curacao with company registration number 159857, with registered address at Zuikertuintjeweg Z/N (Zuikertuin Tower), Curacao ("Company"), licensed in Curaçao under the Licence 365/JAZ Sub-License GLHOCCHKTW0703092022 issued by Gaming Services Provider N.V. for the provision of online games of chance.

SECURITY GOALS AND IMPROVEMENT

This Security Policy describes how Continent Gaming N.V. protects your data and ensures secure operations on betone.com. It applies to all employees, contractors, and third parties involved in providing our services.

The goal of the Company security is to prevent unauthorized access to sensitive data.

Planning of the security system is based on the risk assessment, which allows to provide efficacy of the security controls related to the value of the protected data and relevance of the corresponding threats. To perform risk assessment, evaluate and classify the protected data, identify current security threats. Choose appropriate security controls on the basis of the risk assessment results.

Monitoring of the security controls operation is performed in order to identify security incidents and check the compliance of the actual security controls application with the determined plans for risk processing.

In order to monitor the efficiency of the procedures of security, analyze the relevant records, which show the results of their implementation.

To verify the compliance of the security system with the applicable requirements, perform regular audits (internal or external).

The results obtained are used for the security system improvement. Thoroughly review the identified weaknesses and inconsistencies of the system with the requirements in order to elaborate efficient corrective and preventive actions. The corrective and preventive actions address existing and potential weaknesses of the Company's security, which eventually achieves the main goal: to maintain and improve the quality of data protection.

SECURITY DURING INTERACTION WITH THIRD PARTIES

In each case of interaction with third parties implement measures to mitigate security risks related to a third party. To mitigate the risk of a breach in customers data confidentiality verify third party's trustworthiness and ensure boundaries of the third party's responsibility for the customers data security.

Additionally, we conduct periodic assessments and audits to ensure that all third parties comply with our security requirements and industry best practices. This ongoing oversight helps maintain the integrity and confidentiality of customer data throughout our service ecosystem.

TRAINING

If the Company's employees are not aware of their security responsibilities, the efficiency of the implemented security controls could decrease. Therefore, an atmosphere of responsible attitude to the customers data is the basis for the effective implementation of the security controls. To build the proper atmosphere, awareness of the Company's employees is regularly raised and includes regular reminders to employees about security processes and procedures implemented within the Company.

All new employees undergo mandatory security training as part of their onboarding process to ensure they understand our policies and procedures from day one.

SECURITY OF PERSONAL DATA

We understand the importance of information security and the means needed to protect it. We use reasonable organizational, technical and administrative measures to protect your personal data from unauthorized access or unauthorized modification, disclosure or destruction of information in our possession, and we also take the necessary measures to ensure an adequate level of data security by our subsidiaries, agents, affiliates partners and service providers.

Your personal data is securely stored in a state-of-the-art Tier-IV data center located in Curaçao, which meets the highest international standards for data center infrastructure and reliability. This facility ensures maximum uptime, robust physical security, advanced fire protection, and redundant power and network connectivity to guarantee the continuous safety and availability of your data.

CHANGES TO OUR SECURITY POLICY

We may update this Security Policy from time to time, so please review it regularly.

If there are any material changes to this Security Policy, we will notify you of the changes if required by law. We recommend that you regularly review this page to familiarize yourself with changes to the Security Policy. We will make reasonable efforts to notify you in advance of them by e-mail, through an announcement on the Website or using other communication channels agreed by the parties. We will notify you of the changes in advance, giving you sufficient time to review and understand them before the changes become effective.

CONTACT US

If you have any questions about our Security Policy, please contact us:

- By email: support@continentgaming.com