Cantium Business Solutions

Customer Acceptable Use Policy

Created On: 15/06/22
Created By: Mark Gosden
Internal Ref: V1.01

eis LET'S KEEP IT SIMPLE

KENT-TEACH.COM

1. Introduction

This acceptable use policy ("AUP") defines acceptable practices relating to the use of Cantium's network (the "Network") and /or products or services (the "Service") by customers of Cantium ("Customers") and by users that have gained access to any part of the Service through Customer accounts ("Users"). By using the Service, you acknowledge that you and your Users are responsible for compliance with the AUP. You are responsible for breaches of this AUP by any User that accesses any Service through your account or connection. This AUP applies to all Services provided by Cantium. The provisions of this AUP must hence be read with reference to the Service you are taking from us. In the event of any uncertainty concerning the applicability of any particular part of this AUP to you, please contact us so that we may clarify.

The AUP applies to all aspects of the Service.

"Cantium" means Cantium Business Solutions Limited and all of its affiliates (including direct and indirect subsidiaries and parents). "Cantium Network" includes, without limitation, all equipment, systems, facilities, services and products incorporated or used in such service delivery.

As used in this AUP, "you" refers to Customers, and any reference to "Users" is intended to encompass, as applicable, both Customers and their Users.

This AUP is designed to assist in protecting Cantium, the provided Services, our Users and the wider community as a whole from improper and/or illegal activity, to improve Service and to improve Service offerings. In situations where data communications are carried across networks of other origin (for example, Internet Service Providers (ISPs)) Users of the Cantium Network must also conform to the applicable acceptable use policies of such other ISPs.

2. Rights of Cantium

Cantium requires its customers to comply with Cantium's instructions and all legal, regulatory & best practice requirements relevant to their system, network and any services they may consume. Where a customer fails to meet such requirements, the customer agrees to indemnify Cantium against all losses, expenses, costs (including legal costs) or damages which may be suffered or incurred by Cantium in relation thereto. If Users engage in conduct (or a pattern of conduct), including without limitation repeated breaches by a User whereby correction of individual breaches does not in Cantium's sole discretion correct a pattern of the same or similar breaches, while using the Service that breaches the AUP, or is otherwise illegal or improper, Cantium reserves the right to suspend and/or terminate the Service or the User's access to the Service. Cantium will attempt to notify you of any activity in violation of the AUP and

request that the User(s) cease such activity; however, in cases where the operation of the Cantium Network or Service is threatened we reserve the right to suspend or terminate your Service or the User's access to the Service without notification. In addition, we may take any other appropriate action against you or a User for breaches of the AUP, including repeated breaches wherein correction of individual breaches does not in Cantium's sole discretion correct a pattern of the same or similar breaches. We do not make any promise, nor do we have any obligation, to monitor or police activity occurring using the Service and will have no liability to any party, including you, for any breach of the AUP.

3. Cooperation with Investigations

Cantium will cooperate with appropriate law enforcement agencies and other parties involved in investigating claims of illegal or inappropriate activity. Cantium reserves the right to disclose Customer information to the extent authorised by applicable legal authorities.

4. Modifications to Policy

Cantium reserves the right to amend/modify this AUP at any time without notice. We will attempt to notify Customers of any such modifications either via e-mail or by posting a revised version of the AUP on our website. Any such modifications shall be effective and applied immediately from the date of posting.

5. Prohibited Uses

Illegal Activity

Cantium's Network and Services must be used in a manner that is consistent with their intended purposes and may be used only for lawful purposes. The Service shall not be used for any unlawful activities or in connection with any criminal or civil violation and the Services shall in all cases be used in compliance with applicable laws. Use of the Service for transmission, distribution, retrieval, or storage of any information, data or other material in violation of any applicable law or regulation (including, where applicable, any tariff or treaty) is prohibited. This includes, without limitation, the use or transmission of any data or material protected by copyright, trademark, trade secret, patent or other intellectual property right without proper authorization and the transmission of any material that constitutes an illegal threat, violates export control laws, or is obscene, defamatory or otherwise unlawful.

Unauthorised Access/Interference

A User may not attempt to gain unauthorised access to, or attempt to interfere with, or compromise the normal functioning, operation or security of, any portion of the Cantium Network and / or Service. A User may not use the Service to engage in any activities that may interfere with the ability of others to access or use the Service. A User may not attempt to gain unauthorised access to the user accounts or passwords of other Users for any reason.

6. Responsibilities of Customers

Users are entirely responsible for maintaining the confidentiality of password and account information, as well as the security of their network. You agree to immediately notify Cantium of any unauthorised use of your account or any other breach of security known to you. If you become aware of any breach of this AUP by any person, including Users that have accessed the Service through your account, you are required to notify us without delay.

Cantium accepts no responsibility for the security of Customer systems connected to the Cantium Network or Service. Such security remains the responsibility of the Customer. Where a Customer feels their security / privacy may have been compromised via a system connected to the Cantium Network or Service it is entirely the Customer's responsibility to seek redress from any third parties. Cantium will take all lawful and practicable steps to assist in any such investigation which may be required, subject to the rights of such third parties.

Cantium expects that all Customers and Users of the Cantium Network or Service will undertake best security practices at all times. This includes, but may not be limited to, the following:

1. Any and all accounts used to access the Cantium Network or Service, regardless of type or service they relate to, must be secured with multi factor authentication (MFA).
2. Any and all accounts used to access the Cantium Network or Service, regardless of type or service they relate to, must be configured with a password that meets the NCSC's current minimum recommended standard for password complexity.
3. Any device used to access the Cantium Network or Service must be running a currently supported operating system and be patched and up to date with all available vendor operating system security patches & firmware.
4. Any application used to access the Cantium Network or Service (or, by extension, any application installed on a device that is used to access the

Cantium Network or Service) must be licensed & patched with all available vendor security patches. Applications that are no longer under support / maintenance / license agreement must not be used to access the Cantium Network or Service nor must they be installed on any device used to access the Cantium Network and / or Service.

5. Any device used to access the Cantium Network or Service must be running an up to date and licensed Endpoint Detection & Response (EDR) application. Any device that does not have this or does but the application is not up to date or licensed, is not authorised to access the Cantium Network or Service.
6. Any device used to access the Cantium Network or Service must be running local disk encryption (for example, Bitlocker).
7. Any device used to access the Cantium Network or Service must be connected to a trusted network before access is attempted. Use from public wireless "hot spots" is not permitted unless a trusted VPN service is in use.
8. Any device used to access the Cantium Network or Service must be configured to lock its screen automatically after no more than 5 minutes of device inactivity.

Cantium Customers must not engage in any activity, either lawful or unlawful, which Cantium considers detrimental to its customers, operations, reputation, goodwill or customer relations.

7. Security Event Notifications

All Users of the Cantium Network or Service are responsible for notifying Cantium immediately if they become aware of an impending event that may negatively affect the Cantium Network or Service.

8. Additional Terms and Conditions

The use of the Cantium Network by any Customer of Cantium is subject to the terms and conditions of any agreements entered into by such Customer and Cantium. This AUP is incorporated into such agreements by reference.

9. Complaints and Contact

Any complaints regarding prohibited use or other abuse of the Cantium Network, including breaches of this AUP, should be sent to Cantium. Please include all applicable information that will assist Cantium in investigating the complaint.