Acceptable Use Policy

For virtualDCS services

vmware · Microsoft Tier-1 Cloud Solutions Provider · zadara · NIMBOX · PURESTORAGE

Hewlett Packard Enterprise · NOMINET · DELL · IBM · bsi. ISO/IEC 27001 Information Security Management IS 623296 · HM Government G-Cloud Supplier

VEEAM VCSP Competency — Approved Partner

VEEAM VCSP Reseller Ready — BaaS *for Office 365*

VEEAM VCSP Competency — DRaaS

VEEAM VCSP Reseller Ready — MSP Backup

VEEAM VCSP Reseller Ready — Off-site Backup

This Acceptable Use Policy (“AUP”) describes prohibited uses of the Services offered by virtualDCS and its resellers (the “Services”). We may modify this AUP at any time by posting a revised version on the virtualDCS web site. By using the Services, you agree to the latest version of this AUP. If you violate the AUP or authorize or help others to do so, we may terminate your use of the Services.

No Illegal, Harmful, or Offensive Use or Content. You may not use, or encourage, promote, facilitate or instruct others to use, the Services for any illegal, harmful or offensive use, or to transmit, store, display or otherwise make available content that is illegal, harmful, or offensive. Prohibited activities or content include:

- Illegal Activities. Any illegal activities, including advertising, transmitting, or otherwise making available gambling sites or services or disseminating, promoting or facilitating child pornography.
- Harmful or Fraudulent Activities. Activities that may be harmful to others, our operations or reputation, including offering or disseminating fraudulent goods, services, or engaging in other deceptive practices.
- Offensive Content. Content that is defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable, including content that constitutes child pornography, or depicts non-consensual sex acts.
- Harmful Content. Content or other computer technology that may damage, interfere with, surreptitiously intercept, or expropriate any system, program, or data, including viruses, Trojan horses, worms, time bombs, or cancelbots.ate Subscriber information. We also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this AUP.

No Security Violations. You may not use the Services to violate the security or integrity of any network, computer or communications system, software application, or computing device. Prohibited activities include:

- Unauthorized Access. Accessing or using any System without permission, including attempting to probe, scan, or test the vulnerability of a System or to breach any security or authentication measures used by a System.
- Falsification of Origin. Forging TCP-IP packet headers, e-mail headers, or any part of a message describing its origin or route. This prohibition does not include the use of aliases or anonymous remailers.

No Network Abuse. You may not make network connections to any subscribers, hosts, or networks unless you have permission to communicate with them. Prohibited activities include:

- Denial of Service (DoS). overloading a target with communications requests so the target either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective.
- Intentional Interference. Interfering with the proper functioning of any System

No E-Mail or Other Message Abuse. You will not distribute or facilitate the distribution of unsolicited mass e-mail or other messages ("spam"), including commercial advertising and informational announcements. You will not alter or obscure mail headers or assume a sender's identity without the sender's explicit permission.

Our Enforcement. We reserve the right, but do not assume the obligation, to investigate any violation of this AUP or misuse of the Services. We may investigate violations of this AUP; or remove, disable access to, or modify any content or resource that violates this AUP or any other agreement we have with you for use of the Services. We may report any activity that we suspect violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Our reporting may include disclosing appropriate Subscriber information. We also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this AUP.

Reporting of Violations of this AUP. If you become aware of any violation of this AUP, you will immediately notify us and provide us with assistance, as requested, to stop or remedy the violation. To report any violation of this AUP, please follow our abuse reporting process.