FUJITSU Cloud Service K5: Acceptable Use Policy

Effective as of July 20, 2016

Use of the Cloud Services is subject to this Acceptable Use Policy. Capitalized terms are defined in the 'Fujitsu Cloud Service K5: Terms of Use' document and the Glossary this references.

Application: Each Customer agrees not to engage in or allow End Users to engage in any of activities that are contrary to or prohibited by this Acceptable Use Policy in connection with accessing or using the Cloud Services. Each Customer will (and will each ensure that each End User will also) comply with this Acceptable Use Policy. If a Customer violates this Acceptable Use Policy or authorizes or help others to do so, then Fujitsu may suspend or terminate the Customer's use of the Cloud Services.

Unacceptable Use: Prohibited content, uses and activities include any use of the Cloud Services in a manner that, in Fujitsu's reasonable judgement, involves, facilitates, or attempts any of the following:

- Posting, transmitting, storing, displaying, distributing or otherwise making available any content that is illegal, harmful, offensive, or that violates or encourages the violation of the legal rights of others. Examples of prohibited content include any content that is : (a) threatening, harassing, degrading, discriminatory, hateful or intimidating, or otherwise fails to respect the rights and dignity of others, including other persons or animals; (b) defamatory, libelous, fraudulent or otherwise tortious; (c) obscene, offensive, indecent, pornographic or otherwise objectionable; or (d) protected by copyright, trademark, trade secret, right of publicity or privacy or any other proprietary right, without the express prior written consent of the applicable owner.
- Intentionally distributing any virus, worm, Trojan horse, hoax, time bomb, spyware, corrupted file, computer code, file or program or other item that is of a destructive or deceptive nature, potentially harmful or invasive or intended to damage or hijack the operation of, or to monitor the use of, any hardware, software or equipment.
- Using the Cloud Services for any unlawful, invasive, infringing, defamatory or fraudulent purpose or otherwise harmful act. Examples include stalking, offering or disseminating any fraudulent goods, services, schemes or promotions (for example, pyramid schemes, phishing or pharming), chain letters, child pornography, illegal gaming or gambling, forgery, falsifying or erasing information, impersonating any third party, possession or use of illegal weapons, inciting or enabling suicide, illegal campaigning or electioneering.
- Disabling, interfering with, disrupting or circumventing the operation of the Cloud Services, the servers or networks used to provide these or any other person's use of the Cloud Services. Examples of prohibited activities include: hacking or defacing any portion of the Cloud Service; violating any requirement, procedure or policy of the Cloud Services or their servers or networks; collecting or otherwise obtaining personal data or other information of a third party without consent or by fraudulent means.

- Infringing, violating or misappropriating another's rights, including by removing any copyright, trademark or other proprietary rights notice from the Cloud Services or its servers, networks, software or APIs.
- Obtaining authorized access to, or interfering by any means, with any user, system, network, server, software application or account including by using any robot, spider, site search/retrieval application or other manual or automatic device to retrieve, index, scrape, data mine or otherwise gather Cloud Services content, or reproducing or circumventing the navigational structure or presentation of the Cloud Services or evading filters or otherwise violating the security of integrity of any network or system.
- Using the Cloud Services for any of the following purposes: development, manufacture, use or storage of nuclear weapons; development of nuclear fuel or nuclear source materials or for research regarding nuclear fusion, the development of nuclear reactors or their components or accessories, manufacture of heavy water, or processing or reprocessing of nuclear fuel materials or nuclear source materials; development or manufacture of chemical substances, microorganisms or toxins, rockets or drones, or space research (excluding research related to astronomy) by or for any military or defence agency; or development, manufacture or use of any weapons (including weapons of mass destruction).

High Risk Use: Customer acknowledges and agrees that the Cloud Services are made available for the general use (for example, general office use, personal use and household use) but not for use in connection with any purpose or intended application which involves risks or dangers that could lead to death, personal injury, severe physical or property damage or other loss, or usage for purposes that otherwise requires significant safety precautions ("High Risk Use"), unless the Customer independently takes adequate precautions. Examples of High Risk Use include relying on the Cloud Services for nuclear reaction control in nuclear power facilities, airplane or air traffic control, operation control in mass transport systems, medical equipment for life support or missile launching control in weapons systems. Customers shall not use the Cloud Services in connection with any High Risk Use without properly implementing all appropriate safety precautions required and otherwise appropriate for such High Risk Use. Fujitsu shall not be liable in any way for any claims, losses or other damages relating to any use of the Cloud Services for any High Risk Use.

Compliance with Laws and Regulations: Each Customer is responsible for ensuring that its use of the Cloud Services is in compliance with all applicable laws, statutes, regulations, and codes including laws relating to anti-bribery, anti-corruption and anti-money-laundering including the Bribery Act 2010 and the Foreign Corrupt Practices Act of 1977 ("Relevant Requirements"). The Customer will maintain in place throughout the Term of the Agreement its own policies and adequate procedures to ensure compliance with the Relevant Requirements.

Reporting: If a Customer becomes aware of any violation of this Acceptable Use Policy, the Customer must promptly notify Fujitsu and provide assistance, as requested, to stop or remedy the violation. Fujitsu reserves the right, but does not assume the obligation, to investigate any misuse of the Cloud Services or Service Portal in violation of this Acceptable Use Policy or the other Documentation.

Cooperation with Authorities: Fujitsu may report any activity that Fujitsu suspects violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties, which may include disclosing appropriate Customer and End User information. Fujitsu may also 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 Acceptable Use Policy.

Updates: Fujitsu may modify this Acceptable Use Policy from time to time by posting a new version of this document at the Service Website or at a page accessible to Customers via the Service Portal.