Surecomp

Surecomp Acceptable Use Policy

Last Updated: March 2023

This Acceptable Use Policy (this "Policy") describes prohibited uses of the Software as a Service offered by Surecomp and its affiliates (the "Services"). The examples described in this Policy are not exhaustive. We may modify this Policy at any time by posting a revised version on our website and/ornotifying you in other ways. By using the Services, you agree to the latest version of this Policy. If youviolate the Policy or authorize or help others to do so, we may suspend or 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, fraudulent, infringing, or offensive use, or to transmit, store, display, distribute or otherwisemake available content that is illegal, harmful, fraudulent, infringing, or offensive. You shall be obligated to instruct and ensure any of your end-users (if any) will adhere to the terms of this Policy. Prohibitedactivities or content include:

- **Illegal, Harmful or Fraudulent Activities**. Any activities that are illegal, that violate the rights of others, or that may be harmful to others, our operations or reputation, including disseminating, promoting, or facilitating child pornography, offering, or disseminating fraudulent goods, services, schemes, or promotions, make-money-fast schemes, Ponzi and pyramid schemes, phishing, or pharming.
- **Infringing Content**. Content that infringes or misappropriates the intellectual property or proprietary rights of others.
- **Offensive Content**. Content that is defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable, including content that constitutes child pornography, relates to bestiality, 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, cancelbots or other items of a destructive or deceptive nature.

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 network or computing device (each, a "System").

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.
- **Interception**. Monitoring of data or traffic on a System without permission.
- **Falsification of Origin**. Forging TCP-IP packet headers, e-mail headers, or any part of a

message describing its origin or route. The legitimate use of aliases and anonymous remailers is not prohibited by this provision.

No Network Abuse

You may not make network connections to any users, hosts, or networks unless you have permissionto communicate with them. Prohibited activities include:

- **Monitoring or Crawling**. Monitoring or crawling of a System that impairs or disrupts the System being monitored or crawled.
- **Denial of Service (DoS)**. Inundating 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, including any deliberate attempt to overload a system by mail bombing, news bombing, broadcast attacks, flooding techniques or circumvention of any aspect of the Services.
- **Operation of Certain Network Services**. Operating network services like open proxies, open mail relays, or open recursive domain name servers.
- **Avoiding System Restrictions**. Using manual or electronic means to avoid any use limitations placed on a System, such as access and storage restrictions.
- **Spam**. Using the System to generate, distribute, publish, or facilitate unsolicited mass email, promotions, advertisings, or other solicitations; or
- **Other Surecomp Products**. Using the Services, or any interfaces provided with the Services, toaccess any other Surecomp product or service in a manner that violates the terms of service of such other Surecomp product or service.

Our Monitoring and Enforcement

We reserve the right, but do not assume the obligation, to investigate any violation of this Policy or misuse of the Services. We may:

- Investigate violations of this Policy or misuse of the Services; or
- Remove, disable access to, or modify any content or resource that violates this Policy 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 customer information. We also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigationand prosecution of illegal conduct by providing network and systems information related to alleged violations of this Policy.

Reporting of Violations of this Policy

If you become aware of any violation of this Policy, you will immediately notify us via legal@surecomp.com, and provide us with assistance, as requested, to stop or remedy the violation.