

## **First National Technology Solutions Data Centers Rules and Regulations**

These Rules and Regulations cover: (1) Customer's (and its customers, agents and users) use of and access to FNTS Data Centers and facilities ("Data Centers"); (2) Customer's (and its customers, agents and users) use of the Data Centers online services; and (3) Data Centers maintenance of the services it provides to its Customers.

### **Access to Data Centers**

Only those individuals identified in writing by FNTS on the Customer Registration Form ("Representatives") may access the Data Centers. Customer shall deliver prior written notice to FNTS of any changes to the Customer Registration Form and the list of Representatives. Customer and its Representatives shall not allow any unauthorized persons to have access to or enter any Data Center. Customer and its Representatives may only access that portion of a Data Center made available by FNTS to Customer for the placement of Customer's equipment and use of the Data Center Services (the "Customer Area"), unless otherwise approved and accompanied by an authorized FNTS representative.

### **Use of Data Center Facility**

Customer and its Representatives agree to adhere to and abide by all security and safety measures established by FNTS and set forth in the Customer Guide provided by FNTS to Customer. Customer and its Representatives shall also not do or participate in any of the following:

- Misuse or abuse any FNTS property or equipment or third party equipment;
- Make any unauthorized use of or interfere with any property or equipment of any other FNTS Customer;
- Harass any individual, including FNTS personnel and representatives of other FNTS Customers;
- Engage in any activity that is in violation of the law or aids or assists any criminal activity while on FNTS property or in connection with the Data Center Services.

### **Prohibited Items**

Customer and its Representatives shall keep each Customer Area clean and in good order at all times. It is each Customer's responsibility to keep its area clean and free and clear of debris and refuse. Customer shall not, except as otherwise agreed to in writing by FNTS, (1) store any paper products or other combustible materials of any kind in the Customer Area including card board (other than equipment manuals); and (2) bring any Prohibited Materials (as defined below) into any Data Center. "Prohibited Materials" shall include, but be not limited to, the following and any similar items:

- Food and drink
- Tobacco products
- Explosives and weapons
- Hazardous materials
- Alcohol, illegal drugs and other intoxicants
- Electro-magnetic devices which could unreasonably interfere with computer and telecommunications equipment
- Radioactive materials
- Photographic or recording equipment of any kind including web cameras (other than tape back-up equipment)

### **Scheduled Maintenance**

FNTS will conduct routine scheduled maintenance of its Data Centers and related Services. In the event a mission critical maintenance situation arises, FNTS may be required to perform emergency maintenance at

any time. During these scheduled and emergency maintenance periods, Customer's Equipment may be unable to transmit and receive data and Customer may be unable to access the Customer Equipment. Customer agrees to cooperate with FNTS during the scheduled and emergency maintenance periods.

### **Online Conduct**

Customer acknowledges that FNTS exercises no control whatsoever over the content of the information passing through Customer's site(s) and that it is the sole responsibility of Customer to ensure that the information it and its users transmit and receive complies with all applicable laws and regulations and these Rules and Regulations.

### **Prohibited Uses**

Uses of the FNTS IP Network described below are prohibited. These descriptions are guidelines and are not intended to be exhaustive.

#### *Illegal/Criminal Activity*

The FNTS IP Network may not be used in connection with civil or criminal violations of state, federal or international laws, regulations or other government requirements. Examples of such violations include, but are not limited to: theft, infringement or misappropriation of copyrights, trademarks, trade secrets, or other types of intellectual property; fraud; forgery; theft or misappropriation of funds, credit cards, or personal information; and threats of physical harm or harassment.

#### *Security Violations*

The FNTS IP Network may not be used in connection with attempts - whether or not successful - to violate the security of a network, service, or other system. Examples of these prohibited activities include hacking, cracking into, monitoring, interfering with, or using networks, services or systems without authorization of the owner of the network, service or system; scanning ports; conducting denial of service attacks; and distributing viruses or other harmful software.

FNTS Customers are responsible for maintaining the basic security of their own systems to prevent their use by others in a manner that violates this Policy. Examples of violations of this rule include failing to properly secure a mail server so that it can't be used by others to distribute spam, and failing to properly secure an FTP server so that it can't be used by others to illegally distribute software or other intellectual property. Customers are responsible for taking corrective actions on vulnerable or exploited systems to prevent continued abuse.

#### *Threats*

The FNTS IP Network may not be used to transmit materials of a threatening nature, including threats of death or physical harm, harassment, libel, and defamation.

#### *Offensive Materials*

The FNTS IP Network may not be used for the distribution of offensive materials, including obscene, pornographic, indecent, and hateful materials.

#### *Spam*

The FNTS IP Network may not be used to create or distribute Spam. Spam includes, but is not limited to, any of the following activities:

- Posting a single message, or messages similar in content, to more than five online forums or newsgroups.
- Posting messages to online forums or newsgroups that violate the rules of the forums or newsgroups.
- Collecting the responses from unsolicited email.
- Sending any unsolicited email that could be expected, in FNTS's discretion, to provoke complaints.
- Sending email with charity requests, petitions for signatures, or any chain mail related materials.
- Sending unsolicited email without identifying in the email a clear and easy means to be excluded from receiving additional email from the originator of the email.
- Sending email that does not accurately identify the sender, the sender's return address, and the email address of origin.
- Using FNTS facilities to violate another Internet Service Provider's acceptable use policy and/or terms of service.

Violations of this Policy regarding the distribution of Spam will cause damage to FNTS. Accordingly, Customer shall reimburse FNTS for any costs, expenses and damages incurred by FNTS in the event of violation of this Policy regarding the distribution of Spam, including reimbursement for the costs and expenses related to FNTS employee time necessary to resolve any Policy violations.

### **Indirect Access**

FNTS Customers are responsible for assuring that their customers, agents and users don't violate this Policy. Violations of this Policy by a third party on behalf of an FNTS Customer will be considered a violation of this Policy by such Customer.

In addition, this Policy applies to any email or content transmitted by or on behalf of an FNTS Customer which uses an FNTS account as a mailbox for responses or promotes content hosted or transmitted using FNTS facilities, or which indicates in any way that FNTS was involved in the transmission of such email or content.

The resale of FNTS products and services is not permitted, unless expressly permitted in a written agreement with FNTS.

### **Consequences**

Violations of this Policy may result in a demand for immediate removal of offending material, immediate temporary or permanent filtering, blocked access, suspension or termination of service, or other action appropriate to the violation, as determined by FNTS in its sole discretion. When feasible, it is FNTS's preference to give notice so that violations may be addressed voluntarily; however, FNTS reserves the right to act without notice when necessary, as determined by FNTS in its sole discretion. FNTS, in its sole discretion, may conduct its own investigation of suspected violations of this Policy and may involve, and will cooperate with, law enforcement if illegal or criminal activity is suspected. Violators may also be subject to civil or criminal liability under applicable law. Refunds or credits are not issued in connection with actions taken for violations of this Policy. FNTS has service providers who may be able to take the same or other actions affecting FNTS Customers if this Policy is violated.

### **Incident Reporting**

Any complaints regarding violations of this Policy by an FNTS Customer should be directed to [abuse@FNTS.com](mailto:abuse@FNTS.com). Where possible, include details that would assist FNTS in investigating and resolving the complaint (i.e. expanded headers and a copy of the offending transmission).

**Revisions to this Policy**

FNTS may modify this Policy at any time, effective when posted to FNTS's public web site. Notice may also be provided via electronic mail or regular mail.