Offis Pty Limited
55 Pyrmont Bridge Road
Pyrmont NSW 2009
ABN 70 077 283 811
P (02) 9776 2300
F (02) 8001 1145
W www.offis.com.au
E sales@offis.com.au
ops@offis.com.au

Virtual.Offis
INSTANT IT INFRASTRUCTURE

Acceptable Usage Policy (AUP)

Author

Offis Pty Ltd

Date

Tuesday, August 11, 2009

Version

2.1

Executive Summary

Virtual.Offis is a private company that has been in business since 1992. It provides a complete range of managed services to deliver complex hosting solutions to a rapidly growing number of enterprises since 1997. Virtual.Offis has previously hosted and currently host applications for companies in various industries including telecommunication giants Optus and Vodafone, software vendors Hewlett Packard and Jobpac, OzForex, security company – RSA, and one of Australia's largest merchant bank.

Virtual.Offis provides IBM System I and System X servers, Operating System installation and maintenance, backup routine with retention cycles, premium service 24 x 7 system real-time monitoring and alert response support.

Virtual.Offis hosting solutions include the following Managed Services as standard for a flat monthly hosting fee:

- Operating system maintenance, service pack updates and scheduled patching
- 24 x 7 system monitoring (CPU, HDD & NIC) and alert response. Virtual.Offis technicians are alerted to a problem, respond accordingly and can have it fixed before the customer is even aware of it. Standard alerts are activated for:
    - CPU usage at 90% for 5 min.
    - Memory usage at 90% for 5 min.
    - Disk space at 80%, 90% and 95%
    - Server On-line / Off-line
    - Web site Up / Down with Servers Alive
    - IIS service Stop / Start
    - Monitored SQL Stop / Start
    - Event log tracking for policy changes
- Daily differential & full weekly backups to the central tape library with offsite storage.
- Remote control and secure file transfer via Tivoli IT Management Console.
- Basic protection behind Cisco firewalls prevent common attacks such as Denial of Service (DoS) and synch attacks.
- The firewalls are in stateful failover mode for high availability.
- Disaster recovery and system replication for automated failover.
- Server clustering, server load balancing and geographical load balancing.
- IBM hardware with redundant power supplies, hard drives and standby hardware.
- Real time virus scanning with Symantec Anti-virus and virus definition updates.
- Vulnerability management via a secure portal with links to remediation databases.
- Change management is managed via written authorisation. Customer requested changes may be made over the phone but we will request a confirmation by email.
- Network configuration changes are managed and tracked via Device Expert.

Virtual.Offis has vast experience relating to IBM System I and System X hosting and operations, project planning, network operations and connectivity. We're one of very few infrastructure companies that will offer Managed Disaster Recovery Solutions.

Acceptable Usage Policy (AUP) Definition

This Acceptable Usage Policy specifies the actions prohibited by Virtual.Offis to users of the Virtual.Offis Network. Users may be defined as "customers or anyone who uses or accesses the Virtual.Offis Network or Internet service". Virtual.Offis reserves the right to modify the AUP at any time, effective upon posting of the modified policy to this URL. Any modifications to the AUP will be made when Virtual.Offis feels it is appropriate and it is the user's responsibility to ensure their awareness of any such changes.

Illegal Use

The Virtual.Offis Network may be used only for lawful purposes. Transmission, distribution or storage of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by

copyright, trademark, trade secret or intellectual property right used without proper authorisation, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.

The Network

1. The user acknowledges that Virtual.Offis is unable to exercise control over the content of the information passing over the Virtual.Offis Network. Therefore, Virtual.Offis is not responsible for the content of any message whether or not the posting was made by an Virtual.Offis customer.
2. The Virtual.Offis Network may be used to link into other networks worldwide and the user agrees to conform to the acceptable use policies of these networks.
3. In addition, the user undertakes to conform to the Internet protocols and standards.
4. The user may not circumvent user authentication or security of any host, network, or account (referred to as "cracking" or "hacking"), nor interfere with service to any user, host, or network (referred to as "Denial of Service attacks").
5. Without prejudice to the foregoing, Virtual.Offis considers that any application that overloads the Virtual.Offis Network by whatever means will be considered as making reckless use of the Virtual.Offis Network and as such is not allowed. Use of IP multicast other than by means provided and coordinated by Virtual.Offis is likewise prohibited.
6. Users who violate systems or network security may incur criminal or civil liability. Virtual.Offis will fully co-operate with investigations of suspected criminal violations, violation of systems or network security under the leadership of law enforcement or relevant authorities.

System and Network Security

Violations of system or network security are prohibited, and may result in criminal and civil liability. Virtual.Offis will investigate incidents involving such violations and will involve and will co-operate with law enforcement if a criminal violation is suspected. Examples of system or network security violations include, without limitation, the following:

1. Unauthorised access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorisation of the owner of the system or network;
2. Unauthorised monitoring of data or traffic on any network or system without express authorisation of the owner of the system or network;
3. Interference with service to any user, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks;
4. Forging of any TCP-IP packet header or any part of the header information in an email or a newsgroup posting.
5. Virtual.Offis enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

1. Customer Systems: The Customer may select a custom firewall where specific ports, protocols, and services may be used in accordance with Customer requirements and risk assessments. These request changes are tracked in the call logging system. Customers have SysAdmin level access and therefore can create additional SysAdmin or other privilege level accounts. Virtual.Offis encourages Customers to use least privilege principles. *For more details please review our Security Policy, section AC.*
2. Customer Systems with High Risk and PCI Requirements: Changes to account privileges or firewall rules are documented in the Server Information Package." *For more details please review our Security Policy, section AC.*

NOTE: If approached with complaints relating to any of the above violations, Virtual.Offis will cooperate and assist the police and law enforcing bodies with their investigations in order to bring such misuse and violations to an end.

E-Mail

1. It is explicitly prohibited to send unsolicited mail messages ("junk mail" or "spam") of any kind (commercial advertising, political tracts, announcements) etc.
2. A user shall not use another site's mail server to relay mail without the express permission of the site.
3. Users may not forward or propagate chain letters nor malicious e-mail.
4. A user may not solicit mail for any other address other than that of the user, except with full consent of the owner of the referred address.

Usenet Policy and Posting Restrictions

All users of the Virtual.Offis Network are advised to become familiar with the Virtual.Offis information and guidelines which explain what the service is and how to use it.

Usenet comprises a system of bulletin boards called newsgroups. Usenet access is provided to Internet access customers of the Virtual.Offis network. You may not rapidly open and close or create connections for users other than yourself (our Subscriber). Virtual.Offis Customers will carry newsgroups at their sole discretion. Requests to add a newsgroup from any source, will be evaluated on a case-by-case basis, and added at Virtual.Offis's sole discretion. You must familiarise yourself with the subjects and established guidelines and restrictions of any newsgroup in which you participate and we reserve the right, in our sole discretion, to terminate your Service in the event you violate newsgroup guidelines or restrictions

Users should, before using the service, familiarise themselves with the contents of the following newsgroups: news.newusers.questions; news.announce.newusers; and news.answers Excessive cross-posting (i.e., posting the same article to large numbers of newsgroups) is forbidden. Posting of irrelevant material to newsgroups (also known as USENET spam) is also forbidden. Posting binaries to a non-binary newsgroup is forbidden.

Complaints regarding Illegal Use or System or Network Security issues, Email abuse, USENET abuse or Spamming should be sent to abuse@offis.com.au.

INDIRECT OR ATTEMPTED VIOLATIONS OF THIS POLICY, AND ACTUAL OR ATTEMPTED VIOLATIONS BY A THIRD PARTY ON BEHALF OF AN VIRTUAL.OFFIS CUSTOMER OR A CUSTOMER'S END USER, SHALL BE CONSIDERED VIOLATIONS OF THIS POLICY BY SUCH CUSTOMER OR END USER.