**Computer Virus Policy  
and Information Sheet**

“A virus is a piece of programming code usually disguised as something else that causes some unexpected and usually undesirable event. A virus is often designed so that it is automatically spread to other computer users.”[[1]](#endnote-1) Most viruses are simply nuisances while others do actual damage to a user’s computer, including crashing hard drives, destroying data, and corrupting files.

It is almost impossible to gauge actual dollar damage caused by computer viruses each year[[2]](#endnote-2), but there is no doubt about the time, frustration, and disruption of operations they cause to all kinds of organizations. In a hotel environment the damage can include:

* Interruptions to network access for online registration
* Interruptions to hotel business services (billing, registration, etc.) Interruptions to computer systems access
* Dollar costs for equipment maintenance, consultant fees, network staff overtime, etc.

To protect the operations and assets of the Hotel and ensure that all systems are maximized to the benefit of the employees, the Hotel has implemented, and strongly enforces, this Computer Virus Policy.

This policy pertains to users, including employees, who access the Hotel computer system through direct or indirect sources. This policy also applies to anyone who has the responsibility for managing the Hotel computer environment or any portion of it.

**Responsibilities of the Hotel Information Technology Staff**

* The IT staff will follow industry practices regarding virus protection of Hotel computer resources, but does not guarantee 100% protection.
* Virus scanning software will be installed, updated, and used regularly on servers, workstations, portable computers owned by the Hotel.
* IT Operations will regularly run scan fileservers with software updated daily with new virus definitions and install recommended security patches.
* Since most computer viruses are introduced via electronic mail, virus scanning software will be installed on all Hotel e-mail servers.
* The Hotel will provide instruction and direction to staff in order to raise awareness regarding procedures to be followed to reduce or prevent the possible threat of virus infection.
* The Director of IT Operations will monitor virus developments and ensure that employees have access to the appropriate tools and information to allow protection from viruses.
* IT Operations staff will immediately and thoroughly investigate any report of a possible virus infection so that any possible spread or damage is minimized should the virus be confirmed.
* The Hotel will annually evaluate this policy and perform trend analysis to determine whether this policy and the Hotel-provided anti-virus software and protection measures are appropriate and recommend changes as required.
* The IT General Information Desk will serve as the initial point of contact for all questions and concerns regarding computer virus protection at the Hotel.

**Responsibilities of Hotel Employees**

* Employees are expected to protect personally-owned computers that connect directly or indirectly to the Hotel network by purchasing, installing, and updating virus protection software.
* Any infection or suspected infection must be immediately reported to the IT General Information Desk. No further activities should be performed on the affected computer until the incident has been inspected by an IT staff member.
* Employees are expected to follow common-sense guidelines to protect against viruses distributed via electronic mail, and to make themselves aware of such guidelines by reading the information distributed by IT Operations.
* End users should use extreme caution when downloading information from the Internet. Download only from reputable sites.
* Keep personal use to a minimum on Hotel computers to reduce the possibility of infection.
* All end users are expected to understand the basic functions of virus scanning and protection. This information is regularly distributed by IT Operations.
* All employees should ensure they have backup copies of their individual data, and employees should make regular checks to ensure their data is being backed up via IT Operations. Virus infections can destroy data on an individual computer or network; without proper backups, recovery of destroyed files may be impossible.

**Policy Enforcement**

Bell Orchid Hotel regards any violation of this policy as a serious offense. Violators of the policy are subject to disciplinary action as prescribed in the employee handbooks, including but not limited to revocation of utilization privileges, administrative discipline, or immediate termination of the violator’s relationship with the Hotel. Offenders may be prosecuted under terms prescribed in applicable state and federal laws.

**Further Virus Information**

McAfee Corporation

Virus Hoaxes http://vil.mcafee.com/hoax.asp

Virus Listings http://www.mcafee.com/anti-virus/default.asp

Symantec Corporation

Hoax Listings http://www.symantec.com/avcenter/hoax.html

Latest Virus Threats http://www.symantec.com/avcenter/index.html

Virus Removal Tutorials http://www.symantec.com/techsupp/virusremoval/virusremoval\_info\_tutorial.html

1. http://searchsecurity.techtarget.com/sDefinition/0,,sid14\_gci213306,00.html [↑](#endnote-ref-1)
2. See "Find the Cost of (Virus) Freedom," Wired News, 1/14/02 http://www.wired.com/news/print/0,1294,49681,00.html [↑](#endnote-ref-2)