



# University of Connecticut Health Center

**POLICY NUMBER 2003-45**

**December 1, 2003**

## **POLICY: USE OF SPAM PREVENTION TECHNOLOGY**

### **PURPOSE:**

In order to protect users of UCHC systems from receiving high volumes of offensive and otherwise unsolicited, unauthorized mass marketing e-mails (spam), and to protect the integrity of the UCHC network from vulnerability to virus attacks, the IT Department will maintain and update, as necessary, spam detection and filtering technology.

### **APPLICABILITY**

This policy is applicable to all users of UCHC systems, including employees, faculty, clinicians and students in all UCHC organizational entities (Academic, Research, Clinical, Finance and Administration).

### **SPAM PREVENTION TECHNOLOGY POLICY**

1. The IT Department, at its discretion, will employ state-of-the-art technology to detect and prevent spam e-mails from entering the UCHC e-mail system.
2. The IT Department, at its discretion, will upgrade spam detection technology, as necessary, to ensure it offers up-to-date protection against new spam generation techniques. Broadcast messages will be used to alert UCHC system users of the upgrades.
3. The IT Department will make every effort to prevent the blocking of legitimate business correspondence. However, there is a minor risk that such correspondence will be inadvertently blocked by even the state-of-the-art spam filters utilized by the Health Center. The IT Department will maintain a process to enable UCHC system users to request that specific business-related e-mail addresses be removed from the spam filters for their mailboxes only. Three to four times a year, quarantined spam mail will be made available to e-mail system users for two weeks for this purpose. The User is solely responsible for the determination that the request is a business-related e-mail address.
4. The IT Department will maintain a process to allow individual UCHC e-mail system users to elect to have the spam filter disabled on their mailboxes. The individual making the request will be responsible for ensuring his/her PC has appropriate anti-spam and anti-virus protection. Should a spam-initiated virus subsequently infect the individual's PC and require

IT intervention, or result in any disruption of the network, the individual's network access will be shut down until such time as the virus has been eradicated. Additionally, at the time network access is restored, disabling the network spam filter for that user will no longer be an option.

Sandra Armstrong (signed)

11/24/03

---

**Chief Information Officer**

---

**Date**

Peter Deckers, M.D. (signed)

11/27/03

---

**Executive Vice President for Health Affairs**

---

**Date**

**Replaces: NEW POLICY**