District of Columbia Department of Health **Revoking Privileges After Termination Policy**	**PROCEDURE 720.70** **Implementing Office:** Chief Information Technology Officer **Training Required:** No **Originally Issued:** 12/18/13 **Revised/Reviewed:**
Approved by: _____ Agency Director	**Review by Legal Counsel:** _____ **Effective Date:** 1/13/14 **Valid Through Date:**

I. Authority	Reorganization Plan No. 4 of 1996; Mayor's Order 1997-42; DC Official Code §1-1401
II. Reason for the Policy	To provide guidance to DOH, employees and contractors regarding the revocation of access of any DOH user no longer employed by the agency in order to protect against security threats.
III. Applicability	This policy applies to all DOH employees, contracted staff, volunteers, interns, summer youth employees, and all users of District government Information Technology (IT) resources.
IV. Policy Statement	This Policy describes guidelines and procedures to revoke access for any DOH "User" who is no longer employed by DOH. DOH will revoke employee accounts and access rights to its systems once the employee leaves the organization to protect against security threats in the future, to include access to critical systems through remote access or extranet VPN accounts. DOH reserves the right to review Internet use by DOH employees at any time to determine compliance with this and related policies. Any authorized user who violates this policy may be subject to suspension of service and shall be subject to disciplinary action, up to and including termination.
V. Definitions	User - Any person; including but not limited to DOH employees, third party contractors, temporaries, guests, licensees of DOH, and any person who represents his or herself as being connected to DOH who uses, possesses or has access to DOH communications systems and equipment.
VI. Contents	A. Revocation B. Roles and Responsibilities
VII. Procedures	**A. Revocation:** 1. DOH IT Operations Support is primarily responsible for revoking employee access to DOH information systems in the event of Employee's transfer or termination. 2. DOH will revoke employee accounts and access rights

	to its systems once the employee leaves the organization to protect against security threats in the future, to include access to critical systems through remote access or extranet VPN accounts. 3. It is the responsibility of the outgoing employee's manager and the Human Resources department to notify DOH IT Operations Support when an employee is terminated in order to begin the revocation process. 4. Email or contacting the HelpDesk are appropriate mechanisms to notify DOH IT Operations Support of a request to revoke internet privileges. 5. Upon receiving notification to revoke access either via email or helpdesk ticket, DOH IT Operations Support shall initiate the process of revoking employee access to information systems. 6. Access to systems shall be revoked automatically once the employee ID of the terminated employee is revoked. 7. Revocation of privileges includes the employee's access to all of domains, email, VPN, Extranet and any future access to any DOH computer system. **B. Roles and Responsibilities** 1. Each Senior Deputy Director is responsible for dissemination and enforcement of this policy to their staff. 2. DOH will investigate any alleged or suspected non-compliance with this policy.
VIII. Contacts	Chief Information Technology Officer- (202) 442-4805
IX. Related Documents, Forms and Tools	N/A