September 11th Victim Compensation Fund
Online Claims System Acceptable Use Policy

The U.S. Department of Justice ("DOJ") requires that ALL users of the September 11th Victim Compensation Fund ("VCF") online claims system (also commonly referred to as the "Claimant Portal," the "Online Claim Form," and the "Claims Management System") must comply with the requirements outlined in this document. Failure to comply with these requirements will result in termination of a user's access. The VCF is not required to provide notice before terminating a user's account if the use of the account presents security concerns.

Scope

This policy is applicable to anyone using the VCF online claims system in any capacity.

Enforcement

The DOJ and the VCF will not tolerate any misuse of the VCF's systems and reserve the right to terminate access at any time at DOJ's sole discretion.

Use of any of the VCF's systems or claimant data in any illegal activity may result in an investigation or criminal prosecution.

The VCF online claims system is protected by multiple laws, including, but not limited to, the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030.

Acceptable Use

- Each user must create and use his or her own unique username and password.
- A user's unique username and password **may not be shared with any individual** under any circumstances.
- All users must authenticate each time they log into the system using their own unique username and password.
- Group, shared, or generic accounts and passwords are prohibited. This means you may not log in using another individual's username and password. Users cannot log in with an account that is not their own account.
- Law firm users who have online access to a claim for a VCF claimant whom they no longer represent should immediately contact the VCF to have their access to the claim revoked.
- Law firms must notify the VCF immediately when an employee, contractor, or associate with access to the online claims system leaves the law firm for any reason, or remains at the firm but no longer represents VCF claimants.
- Law firms should review on a quarterly basis the user accounts associated with their firm in the online claims system to ensure that malicious, out-of-date, or unknown accounts do not exist.
- Special care should be exercised with portable devices such as laptops, tablets, and smartphones because the information they contain is especially vulnerable. Sensitive information should be stored in encrypted folders only.
- All users are encouraged to install, run, and maintain up-to-date software that protects their workstation from vulnerabilities and threats associated with malware, trojans, and viruses.
- For additional security, all users are encouraged change their passwords on a pre-defined regular basis that is at least every 90 days.

Unacceptable Use

The activities below are provided as examples of unacceptable use; however the list is not exhaustive. Should a user of the online claims system need to violate these guidelines in order to perform their duties, he or she should contact the VCF to obtain written approval before proceeding.

- Passwords must not be shared with anyone.
- Use of shared, or generic, usernames and passwords is strictly prohibited
- Multiple logins (connections) with the same username and password is prohibited.
- Each user is required, when logged in to the online claims system, to either log off or lock their computer screen when they are away (e.g. do not have visual or physical control) from the computer or their workstations.
- Session sharing is prohibited. A user may not login with their username and password for use or access by another individual, regardless of whether the second individual is authorized or unauthorized.
- Publishing any claimant Personally Identifiable Information or Protected Health Information (PII/PHI) in a publically accessible or insecure location is prohibited.
- All illegal activities, including but not limited to theft, computer hacking, malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or services is prohibited. These also include activities that contravene data protection regulations, activities detrimental to the success of the VCF and/or VCF claimants, as well as sharing sensitive information with anyone who is not authorized to have that information.
- Any activities or actions prohibited by Federal, State, or Local regulation or law, are prohibited.