DC BAR FOUNDATION
WE INVEST IN JUSTICE
DCBF

1420 New York Avenue NW, Suite 650
Washington, DC 20005-6210 www.dcbarfoundation.org
P | 202-467-3750
F | 202-467-3753

INFORMATION SECURITY PROGRAM

(Adopted December 16, 2009)

The District of Columbia Bar Foundation (the "Foundation") is committed to providing loan repayment assistance for lawyers employed in the District of Columbia in nonprofit tax-exempt charitable organizations serving the legal needs of low-income or underrepresented individuals in the District of Columbia. In providing loan repayment assistance, the Foundation obtains from Customers certain Non-Public Personal Information that must be safeguarded consistent with the Foundation's commitment to protecting the privacy of Customers and complying with the requirements of applicable laws, rules and regulations, including the Gramm-Leach-Bliley Act.

This Information Security Program is intended to (1) ensure the security and confidentiality of Customer Information, (2) protect against any anticipated threats or hazards to the security or integrity of such information, and (3) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any Customer.

I. Designation

The Foundation's board of directors is responsible for appointing an Information Security Officer to coordinate this Information Security Program. The Information Security Officer will no less than annually review procedures, propose amendments, and/or take other action as contemplated in this Program. The Information Security Officer is responsible for ensuring that information security processes are consistent with this Program, that there are appropriate security measures and controls in place to protect Customer Information, and that employees understand and comply with their responsibilities hereunder.

II. Risk Assessment

The Information Security Officer must undertake a periodic review to identify potential risks to the security, confidentiality, and integrity of Customer Information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control the risks. The Information Security Officer will assess the likelihood and potential damage that could be caused by the occurrence of these risks and evaluate the adequacy of policies, procedures and controls to mitigate these risks. The contents of this Program have been established and will be periodically updated based upon the findings of this review.

III. Training

The Information Security Officer is responsible for making a copy of this Information Security Program available to employees and for providing appropriate training to employees about privacy requirements generally and this Program in particular.

IV. Compliance

Each employee involved in the administration of the LRAP Programs is responsible for complying with the Foundation's privacy policies restricting the use and disclosure of Customer Information. In particular, no such person may use or disclose such information except as is necessary to perform his or her job responsibilities with the Foundation. In addition, such persons are responsible for understanding and complying with this Program. Without limiting the foregoing, employees should at a minimum follow the practices described below:

a. Do not discuss Customer Information other than in the context of required business.

b. Do not disseminate Customer Information within the Foundation to those without a business need to know and limit the dissemination of documents containing Customer Information to those necessary for the administration of the LRAP Programs.

c. Do not disclose the identity of Customers to anyone inside or outside the Foundation except to the extent necessary to carry out your work-related responsibilities.

d. Keep Customer Information out of view and secure when you are not in your work areas.

e. Do not publicly post or display sensitive Customer Information.

f. Lock files/offices where Customer Information is kept and keep keys in a safe place.

g. Keep checks in a locked area overnight.

h. Set password-protected screen savers to come on after 15 minutes. Do not disclose user IDs or passwords to others except as may be specifically authorized by your supervisor for legitimate business reasons.

i. Shred documents containing Customer Information rather than placing them in trash receptacles.

j. Do not store sensitive Customer Information on portable electronic media.

k. Report immediately any suspected security breach to the Information Security Officer, including suspicious attempts to obtain Customer Information.

Any employee who refuses to comply with this Program or fails to adhere to any policy, standard, or procedure implemented under this Program may be subject to immediate disciplinary action, which may include termination of employment.

V. Violations

Employees are required to report all suspected or known violations of this Program to the Information Security Officer.

VI. Retention and Disposal

When Customer Information is no longer required by the LRAP Programs and is not subject to any data retention policy, law or regulation, it must be disposed of in a manner reasonably designed to protect the confidentiality of this information. For example, hard copies should be disposed of using a paper shredder, and electronically stored information must be irretrievably deleted from systems, databases, e-mail servers, PC hard drives, and other storage devices. When disposing of the electronic media itself (e.g., computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, or any other electronic media or hardware containing Customer Information), data should be irretrievably deleted or destroyed.

VII. Storage

Reasonable measures must be taken and appropriate controls must be in place to secure information systems storing Customer Information. For example,

a. When Customer Information is stored on a server or other computer, access to the computer should require the use of passwords and the computer shall be kept in a physically secure area.

b. User ID and password construction should meet industry best practices (e.g., require the use of at least six characters; upper- and lower-case letters; and a combination of letters, numbers and symbols).

c. Customer information stored in laptops or that can be downloaded to removable media (e.g., USB drives) or portable communication devices (e.g., BlackBerrys) should contain encryption software to prevent the transmission of records and files containing Customer Information.

d. Secure backup records should be maintained, and archived data should be stored off-line and in a physically secure area.

e. All in-bound real-time Internet connections to the Foundation's internal networks should pass through a firewall. Core system infrastructure components such as web servers, electronic commerce and mail servers should not be attached to the Internet unless protected by a firewall.

VIII. Data Transmission

Reasonable measures must be taken and appropriate controls must be in place to ensure the security of inbound and outbound data transmissions between the Foundation and its Customers and internal data transmissions so that information is protected in transit. For example, industry standard enhanced security measures should be employed to encrypt sensitive Customer Information that is transmitted via the Internet.

IX. Failures

Reasonable measures must be taken and appropriate controls must be in place to detect and manage system failures, which shall include the following:

a. Up-to-date and appropriate programs and controls shall be maintained to prevent unauthorized access to Customer Information;

b. Appropriate oversight or audit procedures shall be used to detect the improper disclosure or theft of Customer Information; and

c. Steps shall be taken to preserve the security, confidentiality, and integrity of customer information in the event of a breach.

X. Incident Reporting

Whenever evidence clearly shows that the Foundation has been victimized by a material computer or communications intrusion or breach, an IT investigation will be conducted to obtain sufficient information so that the Information Security Officer can determine what, if any, steps should be taken to ensure that such incidents are unlikely to recur and reestablish effective security measures.

The Information Security Officer is responsible for reporting security breaches involving Customer Information if and as required by applicable law and for determining what, if any, other actions are appropriate under the circumstances. If there are questions regarding the applicable law or which authorities to report to, those should be directed to DCBF's General Counsel.

XI. Definitions

"Customer" means a participant in the LRAP Programs.

"Customer Information" means any record containing Non-Public Personal Information about a Customer, whether in paper, electronic, or other form.

"LRAP Programs" means the District of Columbia Poverty Lawyer Loan Assistance Repayment Program (DC-PLLARP) and the District of Columbia Bar Foundation Loan Repayment Assistance Program (Foundation LRAP).

"Non-Public Personal Information" means personally identifiable financial information that is not publicly available information, including any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable information that is not publicly available information.

"Program" or "Information Security Program" means this Information Security Program.