# Wilson-Bennett Technology Acceptable Use Policy

**10/7/2015**

**Table of Contents**

## Contents

# 1. Policy

Wilson-Bennett Technology is committed to safeguarding the confidentiality and privacy of sensitive data belonging to our customers, employees, vendors, and all other parties doing business with Wilson-Bennett Technology· Sensitive data includes, but is not limited to, Protected Health Information (PHI), social security numbers, bank account information, cardholder data (personal account numbers, PINs, card verification codes, and expiration dates), Cardholder Data Environment passwords, and Wilson-Bennett Technology confidential materials (private business plans, internal network infrastructure, financial information, etc.).

The term “sensitive data” is used throughout this policy to represent all such information.

Wilson-Bennett Technology has implemented this policy to protect the parties listed above by safeguarding this data from intentional and non-intentional misuse, as well as to meet and maintain compliance with laws and industry regulations (namely the Payment Card Industry Data Security Standards – PCI DSS).

**NOTE: Not complying with Wilson-Bennett Technology policies and procedures may be cause for termination of employment from Wilson-Bennett Technology.**

# 2. Scope

This policy applies to all authorized users of Donor Connect.

**Responsibilities**

| **Party** | **Duties** |
|---|---|
| **Users** | Are responsible for exercising good judgment regarding appropriate use of Wilson-Bennett Technology’s assets. |
| | Must review this policy and sign an acknowledgement form with Wilson-Bennett Technology policies upon hire and annually, and be personally aware of their daily responsibility in protecting Wilson-Bennett Technology’s sensitive information. |
| | Consult their Manager or the Compliance Officer with any confusion around their roles and responsibilities and how to apply this policy. |
| | Must never cause a security breach, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or sniffing network traffic. |
| | Must never cause a disruption of service, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes. |

| | |
|---|---|
| | Must never introduce honeypots, honeynets. [A computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems.] |
| | Are not permitted to install wireless access points or modems in the Wilson-Bennett Technology environment without management authorization. |
| | Must not take source and/or original documents out of the office without their Manager's documented approval. |
| | If a user believes that their password has become known, they should immediately change it and then notify their direct supervisor who would then notify the System Administrator. |
| | Do not allow Internet browsers and applications to automatically store passwords. |
| | Let your manager know if your job responsibilities require less or more system access. |
| | If you are ever "locked out" of a system, please use the "Reset Password" link on the login page. |
| | Never open up an email or attachment from an individual or source you do not recognize. If unsure if you should open the email or attachment, contact your direct supervisor for guidance. |
| | Never intentionally introduce malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, keyloggers, and/or any other/new threat. |
| | Are not allowed to disengage or change the anti-virus software installed on network or personal computers used for work without written approval from the IT department. |
| | If personally owned mobile devices are to be used for work, they must be password protected. In addition, ensure the mobile device is set to lock when not active. |
| | Users who wish to utilize other personally owned assets such as a laptop, to connect to the call center specific network, or be used in the activities of campaign administrator or caller duties, must get prior approval from the PCI Compliance Manager. This will be documented using the access control form. Any personally owned laptop used for work must follow the practices outlined in the Data Protection Policy Document. |

- Each party within the scope of this policy as defined above is responsible for following Wilson-Bennett Technology's policies and procedures pertaining to protecting sensitive data and other assets.

## 3. Asset Ownership and Management

- While Wilson-Bennett Technology's stance is to provide a reasonable level of privacy to the user, Wilson-Bennett Technology reserves the right to monitor usages of company such systems including at any time without notifying the user. Wilson-Bennett Technology also reserves the right to withdraw the system at any time without prior notice to the user. All data created on corporate systems remains the property of Wilson-Bennett Technology.

- Wilson-Bennett Technology personnel may review personal owned devices such as mobile devices and laptops periodically that are used for work. Users upon request will provide the mobile device/laptop to a manager and/or a member of the technology team so that they can verify that all policies are being followed. User gives Wilson-Bennett Technology authorization to delete company related data from the personal mobile device/laptop at any time.

- No Wilson-Bennett Technology network and computing asset and/or resource may be used at any time for an unlawful or prohibited purpose. For example, no user may browse, download and upload contents from websites deemed to be malicious.

- For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic. Any software, device or any mechanism that would interfere, disrupt, or evade such monitoring and audit activities is prohibited. Devices that interfere with other devices or users on the Wilson-Bennett Technology network may be disconnected. Firewalls and other blocking technologies must permit access to the scan sources.

# 4. Data Classification & Handling

Information must be protected with security controls commensurate with its sensitivity level. Accordingly, data is to be classified as “sensitive”, “internal use only”, and “public” upon its creation.

Following are descriptions of the three classifications:

**Sensitive:**

Data which would cause irreparable harm to Wilson-Bennett Technology and have financial, competitive, privacy, and legal ramifications, should it be accidentally or incidentally released to internal or external unauthorized individuals.

*All Protected Health Information (PHI), social security numbers, bank account information, cardholder data (personal account numbers, PINs, card verification codes, and expiration dates), Cardholder Data Environment passwords, and Wilson-Bennett Technology confidential materials (private business plans, internal network infrastructure, financial information, etc.) are to be deemed “Sensitive” at all times.*

**Internal Use:**

Data which should be kept from unauthorized access; however would not have grave financial, competitive, privacy, and legal ramifications, should it be accidentally or incidentally released to internal or external unauthorized individuals.

**Public:**

Data which can freely be distributed to all individuals and does not fall within the “Sensitive” and “Internal Use” classifications.

*Examples of “Public” classified items include external client published bulletins, marketing materials in protected format, press releases, public presentations and public announcements.*

Following are the handling guidelines for the three data classifications:

**Sensitive**

Access: Restricted to a business need-to-know and reviewed quarterly.

Third-Parties: An agreement must be signed by a third party prior to obtaining Wilson-Bennett Technology Sensitive assets.

Logging: Access to electronic assets or to secured areas housing sensitive information must be logged and retained for one year.

Security Controls: Anti-virus and file integrity software must be active and current on all systems which handle Sensitive Data. Intrusion detection/prevention systems must be place on network segments in front of the systems, and patch management must be in place.

Email: Sensitive data may never be transmitted over email, unless business necessary, approved by the PCI Compliance Manager and an approved email encryption tool is used.

Such email should be immediately deleted from electronic storage as soon as transmission (outgoing) is complete, unless retention is required and approved by the PCI Compliance Manager for purposes of an ongoing dispute (investigation or cardholder query).

**EXCEPTION: Cardholder data and Cardholder Data Environment passwords may never be transmitted across open access networks which includes end-user messaging such as instant messaging, e-mail, fax, wireless, and text messaging or SMS

Internet: Sensitive data must always be transmitted over a secure and dedicated connection and never in the clear over a public connection. Limit the ability of systems to communicate directly with vendors.

Paper: Sensitive data should not be written or printed on paper, unless it is absolutely necessary to do so for business reasons (this includes facsimile transmissions).

Documentation with Sensitive data must be physically secured from unauthorized access, and shredded as soon as it is no longer needed for business purposes. Sensitive data should not be kept in an open area where unauthorized individuals may view such data.

Electronic Storage: Sensitive data must be either encrypted or truncated when it is stored on any type of electronic media to include, but not limited to, backup tapes, databases, servers, and desktop network computers. Sensitive data may not be processed, transmitted and/or stored on any of the following except if approved by the PCI Compliance Manager and appropriate encryption and passwords are utilized:

- External hard drives Removable flash/media drives
- CD/DVD; Laptop hard drives; Cellular phones

### Internal Use

Access: Restricted to a business need-to-know.

Third-Parties: A Non-Disclosure Agreement must be signed by a third party prior to obtaining Wilson-Bennett Technology assets.

Logging: Access to electronic assets or to secured areas housing Internal Use information must be logged and retained for one year.

Security Controls: Anti-virus and file integrity software must be active and current on all systems which handle Internal Use data. Intrusion detection/prevention systems must be place on network segments in front of the systems, and patch management must be in place.

Email: Internal use data may never be transmitted over email, unless business necessary, approved by the PCI Compliance Manager and/or an approved email encryption tool is used.

Internet: Internal Use data should always be transmitted over a secure and dedicated connection and never in the clear over a public connection.

Paper: Internal Use data should not be written or printed on paper, unless it is absolutely necessary to do so for business reasons (this includes facsimile transmissions). Documentation with Internal Use data should be physically secured from unauthorized access, and shredded as soon as it is no longer needed for business purposes. Sensitive data should not be kept in an open area where unauthorized individuals may view such data.

Electronic Storage: Internal Use data should be either encrypted or masked when it is stored on any type of electronic media to include, but not limited to, backup tapes, databases, servers, and computers.

**Public**

Access: Unrestricted internal and external access.

Third-Parties: An agreement does not need to be signed by a third party prior to obtaining Wilson-Bennett Technology Public information.

Logging: Access to electronic assets or to secured areas housing Public information does not need to be logged.

Security Controls: It is required that anti-virus and file integrity software be active and current on all systems which handle Public information. It is also recommended that intrusion detection/prevention systems be in place on network segments in front of the systems. Patch management must be in place.

Email: Public information may be transmitted over email without the use of an email encryption tool.

Internet: Public information may be transmitted in the clear over a public connection.

Paper: Public information may be written or printed on paper, does not need to be physically secured from unauthorized access, and does not need to be shredded.

Electronic Storage: Public information may be stored in the clear on electronic media of all types.

## 5. Password Management

- Unique user identification to logon to any Wilson-Bennett Technology application and/or network is required.
- Passwords protecting sensitive data must not be easily guessable or easy to crack (must not contain any reference to Wilson-Bennett Technology, real words, birthdates, names of family members, sports teams, pets, etc.).
  a. Passwords protecting sensitive data must be at least eight characters in length.
  b. Passwords protecting sensitive data must contain at least one alphanumeric and/or one special character.
  c. Passwords for new users with access to sensitive data must be set to a unique value, communicated in a secure manner, and required to be changed upon first log-in.
- Passwords protecting sensitive data must never be written down.
- Passwords protecting sensitive data must not be shared with other users, family members, or anyone else (even if asked by the IT Help Desk).
- Repeated input of an incorrect user name/password will lock persons out of a system.
- Passwords must be changed every 90 days.
- Passwords cannot be the same as the last four used (or higher) – including administrator logons. (Does not include third-party controlled applications.)
- A password-protected screensaver must be initiated after 15 minutes (or less) of inactivity for any system with access to sensitive data.
- **Passwords that do not meet the above standards are not acceptable.**

## 6. Physical Access

- Employees surrounding those areas with sensitive data will remain vigilant of unauthorized personnel attempting to gain access, and notify their manager immediately should suspicious activity be observed.

## 7. Testing

- Only Wilson-Bennett Technology-approved software and tools may be used to perform testing, and only authorized individuals may do so.
- No third-party may perform testing of any kind without express permission from the PCI Compliance Manager.

## 8. Copyright Law

- Violating copyright laws is prohibited, including, but not limited to, illegally duplicating or transmitting copyrighted material, for example pictures, music, video, and software from various types of peer to peer file sharing networks.

- Exporting or importing software, technical information, encryption software, or technology must never be in violation of international or regional export control laws.

## 9. Awareness

- At hire and annually, training will be provided on the topics outlined in the Acceptable Use Policy.

## 10. Electronic Communications

- The use of electronic communications (email, Internet, text messages, instant messages, etc.) using Wilson-Bennett Technology systems is intended for business purposes only unless otherwise approved by a direct supervisor and/or the PCI Compliance Manager.

- The following are prohibited activities:

  a. Sending Spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication.

  b. Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.

  c. Use of a Wilson-Bennett Technology e-mail account or IP address to engage in conduct that violates Wilson-Bennett Technology policies or guidelines (including inflammatory, illegal and/or controversial statements).

  d. Posting sensitive or controversial information to a public newsgroup, bulletin board, or listserv with a Wilson-Bennett Technology e-mail or IP address representing Wilson-Bennett Technology to the public.

## 11. Data Breach

A breach is defined as an unauthorized acquisition or reasonable belief of unauthorized acquisition of personal information that compromises the security, confidentiality or integrity of the personal information maintained by a specific entity.

Activities that members of the breach response team will undertake when a data breach is reported:

1. Determine if this breach occurred within our company or is it being reported by an outside entity such as a customer or business partner.

2. Collect Information
   a. Try to determine the extent to what data may have been breached
   b. How many records could be affected
   c. What type of data was breached
   d. Who is involved
   e. When it occurred
   f. Does law enforcement need to be contacted

3. Instruct the person reporting the breach to use all reasonable measures to contain and limit the exposure, preventing further losses while confirming the suspected compromise.

4. Instruct the person reporting the loss not to access the suspected source of compromise.

5. Advise not to turn off the compromised machine if that is the case but instead use every available measure to isolate it from their network if applicable.

6. If this is being reported by an outside entity, let them know that you are there to help and that their reporting this incident is the first step. Tell them that Wilson-Bennett Technology Leadership will contact them later to provide further instructions/ assistance.

7. Report the information you gathered to your direct manager and system administrator as soon as possible. *Escalating this information to the above persons is a critical step*. Each person is required to report this information as soon as the communication with the effected party has ended. The system administrator will contact the PCI Compliance Officer.

8. The PCI Compliance Officer will provide guidance to the business unit manager on contacting the card brands, and sponsoring banks. The PCI Compliance Officer will also, depending upon the circumstances, ask the business unit manager to instruct the merchant or outside entity of applicable next steps… such as applicable regulatory, law enforcement and/or consumer notifications.

## 12. Receipt of Credit Card Data via Email or E-Fax

The receipt of a credit card number via e-mail or e-fax requires that you:

a. Notify your Manager and the PCI Compliance Officer

b. Identify what you received, from whom and what was the method of receipt

c. Do not forward this information via e-mail.

   1) If you need to provide this information to another department at Wilson-Bennett Technology print the communication and the person receiving this will be responsible for shredding the document once the request has been handled.

d. Request that the person avoids sending e-mails and faxes that includes card holder data.

f. Let the person know that you will be deleting the communication that contained the card holder data.

g. Explain to the customer that protecting their private information is important.

h. Securely delete or shred the communication containing the card holder data.