The Interdependence Project Security Policy

Executive Summary

Vision and Philosophy

The Interdependence Project puts securing our donors and event and class participants' personal data as one of the company's highest priorities. We understand that every time we are provided with credit card and bank account information, or other sensitive personally identifying information, they trust that we will protect it—and this policy is designed to ensure that this trust is not misplaced. The foundation of our information security program is a set of strong policies that are in balance with business operational needs.

Security Environment

The Interdependence Project utilizes your data to deliver products and services to our donors and event or class participants. Accordingly, all of your information to include cardholder data as well as other sensitive information will be protected by all staff, contractors, partners and services providers in accordance with well defined policies and procedures.

The Interdependence Project will operate on the security principle of "that which is not explicitly allowed is explicitly denied." Attempts by anyone to access, monitor, use or share information that is not explicitly allowed to them by our security program will be considered a security violation. Further, access to sensitive information will be permitted on a "need to know" basis, such that employees have access to only those data and systems required to perform their assigned jobs. We will deploy systems, processes, policies and training to protect our mission critical data assets and privacy. Most important, we will monitor and enforce compliance to our policies.

Vendor Management

Vendors, partners and other third parties will be required to comply with the same standards established for The Interdependence Project staff. All vendors storing or otherwise accessing our donors and event or class participants' cardholder data must provide proof of PCI DSS Compliance.

Sanctions for Policy Violation

Failure to comply with Security policies and guidelines may result in disciplinary action by The Interdependence Project depending upon the type and severity of the violation, whether it causes any liability or loss to the company, and/or the presence of any repeated violation(s). Each situation will be judged on a case-by-case basis. Sanctions may include termination of employment and / or referral for criminal or civil prosecution, warnings, or additional security awareness training. There is no requirement for advance notices, written or verbal warnings, or probationary periods.

Information Classification, Storage and Destruction

All The Interdependence Project information is categorized into two main classifications: Public and Confidential.

Public information, such as advertising and marketing materials, is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to The Interdependence Project.

Confidential comprises all other information such as sales data, addresses, employee files, etc, that should not be made available outside the company. A subset of confidential information is "Critical Confidential" information that should be restricted to "need to know" access only, such as trade secrets, financial, technical, and personnel information, and other information integral to the success of the company. Sales authorizations containing credit card numbers and cvv2 codes or bank account numbers (PANs), and PANs provided to employees in the course of entering a telephone transaction, fall into the "Critical Confidential" information category.

The Interdependence Project personnel are encouraged to use common sense judgment in securing confidential information to the proper extent. "Critical Confidential" information will be stored in a limited access area (i.e. locked file drawer or safe), and only those employees with a "Need to know" will be provided access to that information. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager.

Under no circumstances is a CVV2 code to be stored, even in paper format. If provided on a paper authorization form, after the transaction is successfully processed, it is to be redacted on all stored documents.

When "Critical Confidential" information in paper form need no longer be stored for any operational or regulatory reason, it must be disposed of via cross-cut shredding or incineration. Any digital information in the "Critical Confidential" category, whether on tape, CD/DVD, or located on a computer hard drive, will be completely erased and rendered unreadable by commercially reasonable methods. (As The Interdependence Project has contracted with a third party for all storage of PANs, none will be stored by the company in digital form.) When feasible, non-critical "Confidential" information should be disposed of in the same manner.

Payment Processing System

The Interdependence Project utilizes a web-based SaaS system provided by PaySimple, a PCI DSS Certified payment processing service provider, for all payment-processing functions. All credit card and ACH transactions, whether authorized over the phone, in writing via mail, or online are transmitted, processed and stored via the PaySimple Solution system. Telephone and online transactions are directly entered into the system. Mailed transactions are entered into the system, and the paper authorization form is then stored in a secure locked cabinet or safe for only as long as required by business operational needs. In no circumstances are PANs stored electronically for any reason—secure storage is completely relegated to the PaySimple system.

The Interdependence Project employees have access to the PaySimple system for processing payments and reporting—but never have access to un-encrypted credit card or bank account numbers. Each User is granted system access permissions based on the minimum functionality required to perform job responsibilities.

During the course of performing their job responsibilities, telephone sales representatives will have access to full credit card numbers, billing addresses, and CVV2 codes. Telephone operators are expressly directed to enter this information directly into the PaySimple system—and are never to record any PANs or CVV2s on paper, nor to repeat or otherwise transmit this information to any third parties.

Access Controls

The Interdependence Project employees will be granted access to sensitive company data and any archived authorizations or reports containing card data or other confidential information on a "need to know" basis. Access to payment processing systems and other company applications will also be granted on the basis of the minimum level required to perform assigned job responsibilities.

Key Access Control Provisions

- Users will only be given sufficient rights to all systems to enable them to perform their job function. User rights will be kept to a minimum at all times.
- A payment processing system Administrator will be responsible for issuing user accounts, provisioning user account permissions and processing limits, and monitoring system usage
- Access to the PaySimple Solution payment processing system will be by individual username and password
- Usernames and passwords must not be shared by users, passwords must be at least 8 alpha numeric characters and should not be written down
- Passwords will expire every 90 days and must be unique over any 360 day period
- User accounts will be locked after 5 consecutive failed logins
- Any paper receipts, reports, or other documents containing card holder data will be secured in a locked file drawer or safe, with access granted on a limited and documented basis. All documents containing card holder data must be checked-out and checked-in by an authorized manager.
- A payment processing system Administrator will be notified of all employees leaving the company and immediately revoke access to all systems and storage facilities

Anti-Virus/Anti-Phishing

The Interdependence Project has implemented {insert anti-virus application name here} for the purpose of computer virus, worm and Trojan Horse prevention, detection and cleanup. In order to ensure the security of our computing environment, all employees using The Interdependence Project computers or systems must adhere to the following:

- All computers accessing company systems, and/or utilizing the PaySimple payment processing system, must use the approved anti-virus/anti-phishing protection software and configuration.
- The virus/phishing protection software must not be disabled or bypassed.
- The settings and automatic update frequency for the virus/phishing protection software must not be altered in a manner that will reduce its effectiveness.
- Employees should NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source.
- Employees should never download files from unknown or suspicious sources.
- Employees should never complete any forms accessed via links embedded in an email from an unknown, suspicious or untrustworthy source.

Acceptable Use

The Interdependence Project is committed to protecting its employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. All computer related systems and equipment including but not limited to computer equipment, software, e-mail accounts, and web browsers are the property of The Interdependence Project. All data obtained during the course of performing job responsibilities is the property of The Interdependence Project. These systems and data are to be used for business purposes in serving the interests of the company, and our donors and event or Class participants' in the course of normal operations. Effective security is a team effort involving the participation and support of every The Interdependence Project employee and affiliate who deals with information and/or information systems. It is the responsibility of every employee know these guidelines, and to conduct their activities accordingly.

Key Acceptable Use Policy Provisions

- Users should be aware that the data they create on the corporate systems remains the property of The Interdependence Project. There is no expectation of privacy or guarantee of confidentiality of information stored on or accessed via any network, computer, or electronic device belonging to The Interdependence Project.

- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. PaySimple payment processing system passwords are changed every 90 days.

- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

- Under no circumstances is an employee of The Interdependence Project authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing The Interdependence Project-owned resources.

- The following activities are strictly prohibited, with no exceptions:

    - Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

    - Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

    - Circumventing user authentication or security of any host, network or account.

    - Providing information about, or lists of, The Interdependence Project employees to parties outside The Interdependence Project.

    - Providing information about or lists of The Interdependence Project donors and event or Class participants', including but not limited to PANs, and other sensitive information, to any external party or unauthorized internal party.

Vendor Management

All vendors that will have access to "Critical Confidential" information, including Credit Card numbers and Bank Account numbers, must be covered by a formal contract that includes the following guarantees:

- Service providers must comply with all PCI DSS requirements, and maintain and provide proof of PCI DSS certification as a service provider.

- Service providers must acknowledge responsibility for security of the cardholder data they possess, including but not limited to:
    - Protect cardholder data as specified by the PCI DSS, if processing or storing payment card data on behalf of The Interdependence Project.
    - Report any known or suspect compromise of that data to the company as soon as possible.
    - Allow for audits by VISA/MasterCard/American Express/Discover or VISA/MasterCard/American Express/Discover-approved entities in the event of a cardholder data compromise.
    - Ensure continued security of cardholder data retained during and after contract terminations.

As part of the Vendor Management program, The Interdependence Project will perform due diligence on each Vendor prior to signing any contract to confirm that the above guarantees have been adequately met.

On at least a yearly basis, The Interdependence Project will review all vendors that have access to "Critical Confidential" information to ensure that:

- PCI DSS compliance certification is up-to-date
- Other procedures in place to protect confidential information continue to adequately protect donors and event or Class participants' and are being properly executed
- Make any changes necessary to policies and procedures