The Gift, Inc. — Our Information Security Policy

The Gift is a gift shop that specializes in handmade crafts from around the world. We have a retail storefront location, and our owner has a home office.

Our business has important reasons for handling personal information. Here is how we use it:

1. As required by law, we keep employment records, including payroll records, and tax forms (W-4 and I-9). We also keep information about the health insurance plan we provide for employees.

2. When a customer pays by check, we ask to see a driver's license or passport, and record the number on the check. We scan the check, endorse it, and deposit at our bank.

3. When a customer pays by credit card, we examine the customer's driver's license or passport, but we don't record the number. We normally don't record the credit card number (we just swipe the card through the reader), but if the reader is broken, we take a manual impression of the card.

Here is how we protect this information:

Designating Our Information Security Manager:
Samantha Hawley, our store manager, is our Information Security Manager (ISM). She keeps this Written Information Security Plan (WISP) updated, trains staff in compliance, and audits staff compliance.

Making Sure Our Vendors are Compliant:
We routinely share Personal Information (PI) in the form of employment records, pension and insurance information, and other information required to be a responsible employer. We share this PI with the state and federal tax authorities, our bookkeeping service, our payroll service, our CPA firm, our legal counsel, and our business advisor. Our computer networking company sometimes may see PI in the course of repair work and consulting. Each January, we require each of these organizations to send us a letter, signed by their CEO or other authorized person, that they follow a Written Information Security Plan (WISP) that fully complies with 201 CMR 17. The only exception is the state and federal tax authorities, which we assume are compliant, since they must comply with laws that are stricter than 201 CMR 17.00.

Ensuring That Our Staff Follows our PI Policy:
Our Information Security Manager (ISM), Samantha Hawley, trains every new member of our staff in his or her role in carrying out the Written Information Security Policy (WISP). This training is refreshed annually. New staff members agree in writing to follow our WISP, and understand that their continued employment in our organization depends on their following the WISP. Employees who fail to follow the WISP are given written warnings, followed, if necessary, by being asked to leave the organization.

A note about the paragraphs that follow: we talk about keeping paper records under lock and key, and computer records restricted to certain users. We use good common-sense practices about this. All restricted documents kept in the home office are kept in a locked

space where it is reasonably safe from burglary and intrusion. If we need a document or a computer file, we hold it closely and don't share inappropriately, and put it back when we're done. For example, we don't leave checks lying out on our desk. Similarly, we don't leave file folders containing W-9 sitting on a table. When we walk away from a computer, we lock the computer by using Windowskey-L.

Protection and Disposal of Paper Records That Contain Personal Information (PI)
All paper records that have PI are kept under lock and key in the store office or in the owner's home office. We destroy obsolete records using an office-grade shredder. Records containing PI are only taken from the store or the home office when necessary for business reasons. If staff does this, they must explain in writing to the ISM why this is necessary. PI may be faxed, mailed, or delivered to compliant vendors and customers. PI is never emailed, unless using the encryption methods described below.

When we receive checks from customers, we scan them and keep a copy in a computer directory that can only be accessed by our AR staff, which is our store manager, Samantha Hawley, our bookkeeping service, and our CPA firm. The checks are kept under lock and key until they are deposited in the bank by our store manager or her assistant, James Sorkin.

Employment Paper Records are Restricted
Paper employment records are kept under lock and key, and accessed only by the staff responsible for employment issues, which in our case is the store manager, Samantha Hawley, and the owner, Virginia Eckhart.

Employment Computer Records are Restricted
Computer employment records are kept in a Secure Computer Network, and are similarly restricted. See "Secure Computer Network" below for our practices for keeping our computer network secure.

We Never Email Personal Information (PI), Except in Strong Encrypted Form
We don't allow Personal Information (PI) to be included in plain email between us and our payroll and pension companies, accountant, and bookkeeper. When we do need to send PI via email, we use Strong Encryption with a password arranged in person or by fax or telephone.

The Methods We Use for Strong Encryption
We utilize encryption software to and passwords that can unlock those encrypted files are Strong Passwords.

Our Strong Password Policy
Our Password Policy: passwords of at least 8 characters, including one symbol, one number and one change of case. The password must be hard to crack by a dictionary attack, so if it has a word or proper name, it must have at least TWO unconnected words and proper names.

We change user passwords annually. We accept the reality that co-workers will often learn one another's passwords, even though we discourage this, so we also change all user passwords when an employee leaves.

We Do Not Keep Personal Information (PI) on Portable Devices, Except in Strong Encrypted Form
We do not keep PI on laptops, or other handheld or portable devices. We store backups on external hard drives and flash drives, encrypted with Strong Passwords using Strong Encryption.

How We Secure Our Network to Make It Safe for Personal Information (PI)
Our computer network is a Secure Network. We follow the advice of our computer networking firm for security. As such our Firewall has Gateway security services and is reviewed atleast annually. Passwords changed when staff leaves. Our Wireless is encrypted atleast 128bit. Strong Passwords, multiple attempt lockout. Antivirus kept up to date both in version and in signatures. Remote access is only by remote access software that is encrypted and secure.

When a Staff Person Leaves Our Organization, We Block His/Her Access to Computer Systems and Paper Records
When a staff person leaves our organization, all passwords that person used are changed, so that the person no longer has access to our computer network remotely or if s/he visits the office. The person also returns any keys used to physically secure PI.

Computer backups tapes are encrypted with a strong password. We keep regular backups on and offsite, and test them regularly.

If a Breach Occurs
If our ISM determines that PI has been accessed without authorization, she will notify the Office of Consumer Affairs & Business Regulation (OCABR) and the Attorney General's Office, describing the theft in detail, and work with authorities to investigate the crime and to protect the victim's identity and credit. To the extent possible, our ISM will also warn the victims of the theft so that they can protect their credit and identity.