Winter Greenhouse Information Handling Policies

Winter Greenhouse is the sole owner of information collected in their local retail store and on their websites. In order to protect the information assets that Winter Greenhouse handles, to ensure the privacy and security of its customers, to meet statutory, regulatory and contractual obligations, and to ensure the highest reputation, Winter Greenhouse has defined these Information Handling Policies.

These policies apply to all Winter Greenhouse employees, relevant suppliers, contractors and freelancers. Compliance with this Policy is mandatory. Employees are required to read these Information Handling policies and verify that they understand them by signing an acknowledgement form (see Appendix 10.1). Failure to comply may result in disciplinary action, dismissal or contract termination.

Revision	Effective Date	Written By	Reviewed By
1.0	Nov13, 2020	Ole Hoppe	Jim Wilson
1.1	Nov21, 2020	Ole Hoppe	Jim Wilson

Table of Contents

1 Privacy Policy....3
1.1 Purpose....3
1.2 Scope....3
1.3 Policy....3
1.3.1 Collecting Personally Identifiable Information....3
1.3.2 Using Personally Identifiable Information....3
1.3.3 Cookies and User Tracking....3
1.3.4 Sharing Personally Identifiable Information....4
1.3.5 Updating Personally Identifiable Information....4
1.3.6 Protecting Personally Identifiable Information....4
1.3.7 Children's Privacy....4
2 Ethics and Acceptable Use Policy....5
2.1 Purpose....5
2.2 Scope....5
2.3 Policy....5
2.3.1 Ethics....5
2.3.2 General Use....5
2.3.3 Unacceptable Use....5
3 Storage Policy....7
3.1 Purpose....7
3.2 Scope....7
3.3 Policy....7
3.3.1 Physical Security....7
3.3.2 Availability....7
3.3.3 Loss Prevention....7
3.3.4 OS Permissions and Encryption....7
3.3.5 Protection from Malware....7
3.3.6 Retention and Destruction....8

4 Transfer Policy....9
4.1 Purpose....9
4.2 Scope....9
4.3 Policy....9
4.3.1 Transfer via Internet....9
4.3.2 Transfer on the Intranet....9
4.3.3 Transfer on Mobile Devices....9
5 Access Control Policy....10
5.1 Purpose....10
5.2 Scope....10
5.3 Policy....10
5.3.1 Role-Based Access Control....10
5.3.2 Password Rules....10
5.3.3 Account Lockout....11
5.3.4 Screen Lock....11
5.3.5 SSH Authentication....11
6 Log Management Policy....12
6.1 Purpose....12
6.2 Scope....12
6.3 Policy....12
6.3.1 Logs to Gather....12
6.3.2 Access Control to Logs....12
6.3.3 Automated Monitoring and Triggering of Investigative Alarms....12
7 Incident Response Policy....13
7.1 Purpose....13
7.2 Scope....13
7.3 Policy....13
7.3.1 Preparation....13
7.3.2 Identification....13
7.3.3 Containment....13
7.3.4 Eradication....14
7.3.5 Recovery....14
7.3.6 Lessons Learned....14
8 Definitions....15
8.1 Personally Identifiable Information....15
8.2 Sensitive Information....15
8.3 Information Security Incident....15
8.4 Online Marketplace....15
9 Policy Maintenance....17
10 Appendices....18
10.1 Agreement to Comply with Winter Greenhouse Information Handling Policies....18

1 Privacy Policy

1.1 Purpose

This policy describes Winter Greenhouse's views and procedures on the information collected from customers and website users.

1.2 Scope

This policy applies to all information collected from Winter Greenhouse customers and website users, as well as all Winter Greenhouse management and staff handling such information.

1.3 Policy

Winter Greenhouse is collecting information from its customers and users on its websites and in the local retail store as one of its business activities to provide them with best possible products and services.

1.3.1 Collecting Personally Identifiable Information

The information collected includes Personally Identifiable Information (PII). It is collected by forms on our websites or during checkout at our local retail store or over the phone.

We are also collecting information about our customers' devices like operating system and browser type. This information is automatically recorded in our servers' log files.

1.3.2 Using Personally Identifiable Information

We use this information to:

- send our newsletters
- send our printed catalog
- sign-up for an event
- provide personalized special offers and services
- get paid for our products and services
- contact regarding purchases
- ship products ordered
- prevent misuse of our websites

Information about our users' devices helps us identify issues with our website software and improve on the experience with our websites.

1.3.3 Cookies and User Tracking

Our websites make use of cookies, small text files placed on our users' devices, which allow us to distinguish one from another, and enable us to individualize and optimize our users' experience with our websites.

We currently do not use any user tracking technology except the default server logs.

1.3.4 Sharing Personally Identifiable Information

In general Winter Greenhouse will not sell, rent or share PII to any outside parties with the following exceptions:

- To get paid we need to share PII by securely forwarding it to our payment provider. We do not store credit card information.
- To ship an order we need to share PII by securely transferring it to our shipping label providers (USPS, FedEx).
- We may have to comply with requests from government agencies to share PII during legal processes.

The mentioned outside parties are required to keep confidential any information received on behalf of Winter Greenhouse.

1.3.5 Updating Personally Identifiable Information

Our customers can update their information or request account deletion

- by requesting the changes while at our local retail store
- by calling 715-266-4963 (Winter Greenhouse) or 715-200-5234 (Miniature Gardening)
- by sending their request to info@wintergreenhouse.com or info@miniature-gardening.com
- by updating their account information at miniature-gardening.com
- by following the unsubscribe link in each newsletter to opt out of future issues

1.3.6 Protecting Personally Identifiable Information

Winter Greenhouse is committed to protect PII from unauthorized access, use, transfer or disclosure by

- ensuring ethical behavior and only proper, controlled use
- controlling physical access to servers
- limiting access to those with a need to know
- implementing network controls to prevent unauthorized access from public networks
- storing and transferring in encrypted form (using AES-256 and TLS 1.2)
- secure, irrecoverable disposal when no longer needed
- automated monitoring of our network for suspicious activity
- following up on any incident to mitigate any adverse effect and prevent it from occurring again

1.3.7 Children's Privacy

Winter Greenhouse does not knowingly collect information from children under the age of 13 and does not target its websites to children under 13. We encourage parents and guardians to take an active role in their children's online activities.

2 Ethics and Acceptable Use Policy

2.1 Purpose

This policy is to ensure ethical conduct and to make all individuals with access to computing devices and information assets maintained by Winter Greenhouse aware of the limits existing for their use of these devices and assets.

2.2 Scope

This policy applies to all individuals working at Winter Greenhouse and to all computing devices and information assets they are accessing as part of their job duties.

2.3 Policy

2.3.1 Ethics

Ethical conduct must be the basis for working at Winter Greenhouse under all circumstances.

2.3.2 General Use

All employees may access, use, transfer or share information maintained by Winter Greenhouse only to the extent it is authorized and necessary to fulfill their assigned job duties.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult their manager.

For network maintenance purposes and to ensure compliance with this policy, authorized individuals within Winter Greenhouse may audit or monitor equipment, systems and network traffic at any time.

When using Winter Greenhouse resources to access and use the Internet, users must realize they represent the company. Unless posting is in the course of business duties, postings by employees from a Winter Greenhouse email address to newsgroups or social media must contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Winter Greenhouse.

2.3.3 Unacceptable Use

Under no circumstance is Winter Greenhouse staff authorized to engage in any activity that is unethical or illegal under local, state, federal or international law while utilizing resources owned by Winter Greenhouse. And no-one should influence others to do so. An employee should report any dishonest or damaging activities to their manager.

The following activities are, in general, prohibited. Employees like IT staff may be exempted from these restrictions during the course of their legitimate job responsibilities. These activities are examples, the list is by no means exhaustive.

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation of software products that are not appropriately licensed for use by Winter Greenhouse.
- Accessing Winter Greenhouse owned devices and information assets for any purpose other than conducting Winter Greenhouse business, even if the employee has authorized access.

- Introduction of malicious programs into the network (like viruses, worms, Trojans).
- Revealing one's account password to others or allowing use of one's account by others. This includes family and other household members when work is being done at home.
- Using a Winter Greenhouse device to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products or services originating from any Winter Greenhouse account.
- 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.
- Port or security scanning except after prior notification to the IT department.
- Executing any form of network monitoring which will intercept data not intended for the employee's host.
- Circumventing user authentication or security of any device, network or account.
- Interfering with or denying service to another network user (e.g. Denial of Service (DoS) attack).
- Providing information about or lists of Winter Greenhouse employees to parties outside Winter Greenhouse.
- Sending unsolicited email messages like advertising material to individuals who did not specifically request such material.
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any email address other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Blogging by employees, whether using Winter Greenhouse’s systems or personal devices, is also subject to the terms and restrictions set forth in this policy. Limited and occasional use of Winter Greenhouse’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Winter Greenhouse’s policy, is not detrimental to Winter Greenhouse’s or its employees' best interests, and does not interfere with an employee's regular work duties. Blogging from Winter Greenhouse’s systems is also subject to monitoring.
- Employees are prohibited from revealing any Sensitive Information when blogging.

3 Storage Policy

3.1 Purpose

This policy describes for Winter Greenhouse's information storage systems the physical, technical and administrative controls established to ensure information

- **integrity**: prevent tampering with data
- **availability**: minimize the risk of data getting destroyed or becoming inaccessible

3.2 Scope

This policy applies to all computing devices involved in storing information assets maintained by Winter Greenhouse as well as all individuals with access to these devices and assets.

3.3 Policy

Credit card details must never be stored on Winter Greenhouse's information storage systems. When accepting an order over the phone and receiving credit card details they must be entered directly in one of the available checkout systems for a one time payment only.

3.3.1 Physical Security

Winter Greenhouse's information storage systems (e.g. computers or filing cabinets storing Sensitive Information) are protected from unauthorized physical access by being located in rooms locked securely.

3.3.2 Availability

To minimize risks to information availability, Winter Greenhouse information storage systems are protected by:

- RAID (redundant disks)
- uninterruptible power supply
- backup power generator
- a backup web server maintained in warm standby mode

3.3.3 Loss Prevention

Against information loss Winter Greenhouse maintains

- two independent backup copies with multiple snapshots on each copy
- access to backup available for each user via drive mounted read-only in file manager
- one additional backup in a remote building
- multiple snapshots of web server backup

3.3.4 OS Permissions and Encryption

Winter Greenhouse stores Sensitive Information protected by Operating System (OS) permissions or when required e.g. by Online Marketplace policies in AES-256 encrypted directories.

3.3.5 Protection from Malware

Servers have anti-malware software installed which is scanning all relevant drives weekly, and any file

that is created or changed is scanned instantly as well. Each email is also scanned.

Workstations have anti-malware software installed which is scanning all relevant drives weekly, and also removable drives instantly when inserted.

Malware definition files are updated daily.

3.3.6 Retention and Destruction

Winter Greenhouse retains Sensitive Information only as long as required. Originals and any copies are securely purged from the storage systems when the time for destruction has come and in a way that renders the information irrecoverable.

4 Transfer Policy

4.1 Purpose

This policy describes Winter Greenhouse's physical, technical and administrative controls that ensure Sensitive Information is transferred securely between different devices and storage locations.

4.2 Scope

This policy applies to all computing devices involved in transferring Sensitive Information maintained by Winter Greenhouse as well as all individuals with access to these devices and information.

4.3 Policy

In general any individual transferring Sensitive Information has to make sure it is done in a manner that doesn't allow unauthorized access e.g. by sufficiently encrypting the information.

4.3.1 Transfer via Internet

Winter Greenhouse transfers Sensitive Information via Internet

- by using HTTPS protocol with TLS 1.2 encryption
- through AES-256 encrypted SSH tunnels

Attempts to use unencrypted channels (FTP, HTTP) are either not possible or are automatically converted to a secure method.

Sensitive Information must not be sent via unencrypted email.

4.3.2 Transfer on the Intranet

The transfer mechanisms applied for transfer via Internet are also applied to the transfer on the Intranet.

All wireless (local WiFi) connections are WPA2-Personal (AES) encrypted.

4.3.3 Transfer on Mobile Devices

Sensitive Information must not be transferred on mobile devices or storage media.

5 Access Control Policy

5.1 Purpose

This policy describes for Winter Greenhouses' information assets the physical, technical and administrative controls established to ensure information

- **confidentiality**: prevent unauthorized access to information assets and all supporting infrastructure

5.2 Scope

This policy applies to all computing devices involved in storing information assets maintained by Winter Greenhouse as well as all individuals with access to these devices and assets.

5.3 Policy

5.3.1 Role-Based Access Control

Roles must be defined for the fulfillment of different job functions. Each role must be granted access to computing devices and information assets with least privilege to meet that role's need-to-know.

Individuals must be assigned to these roles as required. An individual may not share their access privileges with anyone else. An individual must immediately be unassigned their roles when there is no more requirement, e.g. when the individual is leaving the company. Individuals' access privileges must be reviewed once a year.

When hiring individuals with access to Sensitive Information job-related background checks must be conducted by a third-party agency to collect information about education, past employment, finances, character and reputation. All information obtained will only be used to support the employment process and will be kept strictly confidential. These background checks are conducted and applicant information collected, stored and disposed of in compliance with all applicable federal and state laws and regulations.

5.3.2 Password Rules

Create a Strong Password

- at least 10 characters
- use capital and small letters, digits and special characters
- change once a year

Password strength testers like my1login value a word broken into two parts by a special character, so the two parts are not dictionary words, with a number appended separated by another special character. This is memorable and highly secure.

Example: **Mem^ory-842**

Do Not Reuse Passwords

A hacker finding out the password for one account would gain access to all other accounts secured by the same password.

Maintain a Master Password Document

To keep track of many different passwords, create one master password document e.g. with LibreOffice and save it with a master password. (LibreOffice then uses AES-256 encryption.)

5.3.3 Account Lockout

More than 6 attempts to login with the wrong password must lock an individual out for 30 minutes.

5.3.4 Screen Lock

Computer screens potentially displaying Sensitive Information must be locked automatically, e.g. by starting a screen saver, after 10 minutes of inactivity, and require the user's login password to unlock.

5.3.5 SSH Authentication

For Secure Shell (SSH) access e.g. to remote servers password authentication must be disabled, only public key authentication must be possible. "root" access must be restricted to known good IP addresses.

6 Log Management Policy

6.1 Purpose

This Policy is about defining logs to gather in order to detect security-related events, access control to these logs, automated monitoring to detect suspicious activity, and triggering of investigative alarms.

6.2 Scope

This policy applies to all applications and systems managing Sensitive Information as well as all individuals with access to these applications and systems.

6.3 Policy

6.3.1 Logs to Gather

- Operating System Logs: Ubuntu Server systemd-journald service
- Web Server Logs: Apache HTTPD Server access and error logs
- Intrusion Prevention Logs: Fail2ban and Suricata logs
- Application Logs: User logins and duration

All logs must be retained for at least 90 days.

6.3.2 Access Control to Logs

The logs described above must only be accessible to privileged system maintenance accounts like "root".

6.3.3 Automated Monitoring and Triggering of Investigative Alarms

- **SSH Intrusion Attempts**: Any successful SSH login originating from an unknown IP address must promptly be reported to the system administrator.
- **Network and Application** Intrusion **Attempts**:
  - OSSEC must be configured to monitor all available logs, alert about intrusion attempts via email to the system administrator, and respond actively in real time to major threats e.g. by blocking communication with an offending host for at least 10 minutes.
  - After 6 attempts to login with the wrong password the user must be prevented from further attempts for at least 30 minutes, and the system administrator must receive an alert.

7 Incident Response Policy

7.1 Purpose

This policy defines roles, responsibilities, procedures and reporting requirements to efficiently deal with different types of Information Security Incidents (ISI) to mitigate their effects and prevent them from reoccurring.

7.2 Scope

This policy applies to all applications and systems handling Sensitive Information as well as all individuals with access to these applications and systems.

7.3 Policy

7.3.1 Preparation

The Information Security Officer (ISO), Jim Wilson, is responsible for communicating security policies to employees, contractors and business partners, and for ensuring the adherence to these policies. In case of a suspected ISI, the ISO must decide if this Incident Response Policy needs to be applied and must drive its execution. Any changes to the Incident Response Policy must be reviewed and approved by the ISO.

The System Administrator (SA), Ole Hoppe, is responsible for maintaining and monitoring the information systems, for alerting the ISO of any suspected ISIs and for giving him advice when deciding on them. The SA is also responsible for containing, eradicating and recovering from an ISI, as well as for suggesting improvements following the analysis and documentation of an ISI.

Every employee is responsible for alerting the ISO of any suspected ISIs.

All employees and managementwill be trained annually to maintain awareness of potential information security threats and to prevent certain types of attacks.

7.3.2 Identification

The ISO together with the SA will determine if the suspected ISI actually qualifies as such. If confirmed, the SA will determine the scope of the compromise.

7.3.3 Containment

To prevent more damage, depending on the type of ISI

- the SA will isolate the affected systems e.g. by disconnecting them from the network
- to isolate a web server the SA will download a complete backup and shut the web server down
- the SA will block the IP address(es) of offending traffic in the firewall configuration
- all passwords of all systems connected to the compromised systems will be changed by the responsible people
- the SA will inform business partners like Online Marketplaces within 24 hours of detecting the ISI if their Sensitive Information is affected
  - Amazon via email to 3p-security@amazon.com

- the ISO will not notify any regulatory authority, nor any customer, on behalf of Amazon unless Amazon specifically requests in writing that he does so; Amazon will be given the opportunity to review, and unless such notification is required by law approve, form and content of any notification to any party
- the ISO will inform the card owner and relevant third parties like VISA Fraud Control and law enforcement
- the ISO will inform business partners like Online Marketplaces within 24 hours if their data is being sought during legal processes or by applicable law

7.3.4 Eradication

To eliminate the root cause of the compromise

- the SA will restore the backup of an affected web server to a local, stand-alone machine
- the SA will examine the affected systems to determine when, how, and where the ISI originated
- if it is reliably possible to clean the affected systems
  - the SA will purge malware from the affected systems
  - the SA will restore lost/damaged files from backup
- if it is not reliably possible to restore the affected systems
  - the SA will rebuild the affected systems from scratch
  - the SA will restore data from a reliable backup copy
  - the SA will restore missing data as far as possible manually from the compromised systems carefully ensuring their integrity
- the SA will fix the vulnerability that allowed the exploit in web app code or configuration or by upgrading a software component
- the ISO will have fraudulent credit card transactions reversed
- the ISO will dismiss an offending employee

7.3.5 Recovery

To restore affected systems to normal operation

- the SA will reconnect isolated devices to the network again
- the SA will upload a reliably cleaned backup copy overwriting an affected web server
- the SA will especially closely monitor restored systems during the first weeks of operation
- the SA will replace a stolen/lost device
- the ISO will hire a new employee to replace a dismissed one
- employees will be reminded of the dangers of malicious mail and websites

7.3.6 Lessons Learned

When everything is up and running again, the SA will complete the incident's documentation after thorough analysis to improve on policies, harden systems, and upgrade other preventive measures to avoid future similar compromises.

8 Definitions

8.1 Personally Identifiable Information

Personally Identifiable Information (PII) is information that contributes to making a person identifiable:

- name
- physical address
- email address
- telephone number
- credit card details
- IP address

8.2 Sensitive Information

Sensitive Information needs to be protected from unauthorized access to prevent disadvantage to an individual or organization.

This includes, but is not limited to

- **Personally Identifiable Information**
- **Access Credentials** like user name and password
- **Business Secrets** like suppliers, clients, employee information, financial information, schedules, technology

8.3 Information Security Incident

This is an event that compromises the **Confidentiality**, **Integrity** or **Availability** (**CIA**) of an information asset. This can be a deliberate, malicious attack or an involuntary accident. The following are common types of security incidents:

- **Malware**: malicious software (virus, worm, Trojan horse, adware, ransomware, etc.)
- **Phishing and Social Engineering**: type of email attack attempting to trick users into divulging credentials, downloading an attachment with malicious code, or visiting a website that installs malware on their system
- **Denial of Service (DoS) Attack**: a system, usually a Web server, is flooded with so much traffic that legitimate users can no longer access it
- **Web App Attack**: e.g. specially crafted URLs or entries into forms e.g. of an online store allow an attacker to gain access e.g. to Personally Identifiable Information by exploiting vulnerabilities via buffer overflows, SQL injection, cross-site scripting, etc.
- **Loss or Theft of Devices**: that contain corporate information or that can access corporate networks
- **Insider Attack**: e.g. disgruntled employees may misuse their privileges potentially even evading company's security measures with their insider knowledge

8.4 Online Marketplace

This is marketplaces on the Internet where Miniature Gardening is advertising on like

- Amazon
- eBay
- Etsy
- Houzz
- Walmart

9 Policy Maintenance

These policies will be reviewed every 6 months or after a major system change.

These policies will be published on Winter Greenhouse's websites and customers notified whenever there are any changes.

10 Appendices

10.1 Agreement to Comply with Winter Greenhouse Information Handling Policies

I have read and understood this policy document and agree to follow it.

Name	Signature	Date