Vandelay Industries
Acceptable Usage Policy
Siddesh R Jaadhav, Subash Reddy Karra, Snigdha Lal,
Dan Mishel, Siobhan O'Neill, and Ben Orga

1 Overview

The purpose of this policy is to establish the acceptable and unacceptable use of electronic devices and network resources at Vandelay Industries. This policy is to be used in conjunction with Vandelay Industries established culture of ethical and lawful behavior, openness, trust, and integrity.

Vandelay Industries provides computer devices, networks, and other electronic information systems to employees and other authorized users in order to meet missions, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires the users of information assets to comply with company policies and protects the company against damaging legal issues.

2 Scope

The scope of this policy covers all computing resources include all company owned, licensed, or managed hardware and software, and use of the network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network. This policy applies to information assets owned or leased by Vandelay Industries, or to devices that connect to a Vandelay Industries network or reside at a Vandelay Industries site.

All employees, contractors, consultants, temporary and other workers at Vandelay Industries, including all personnel affiliated with third parties must adhere to this policy.

Information Security must approve exceptions to this policy in advance. Employees, contractors, consultants, temporary and other workers must request an exception to this policy through their appropriate management chain including approval from their division manager.

3 Policy Statement

3.1 General Requirements
3.1.1 As an employee of Vandelay Industries and in accordance with Vandelay Industries’ policies, standards, and guidelines, it is your responsibility for exercising good judgment regarding appropriate use of Vandelay Industries’ resources. It is strictly prohibited to use Vandelay Industries’ resources for any unlawful or excluded purpose.

3.1.2 Authorized personnel may monitor and audit equipment, systems, and network traffic, following the Audit Policy, in order to uphold security, compliance, and maintenance purposes. Any devices interfering with other devices or users on the Vandelay Industries network may be disconnected. Information Security prohibits actively blocking authorized audit scans. Firewalls and other blocking technologies must permit access to the scan sources.

3.2 System Accounts

3.2.1 You have access to use only the computers, computer accounts, and computer files for which you have authorization. You have the responsibility for the security of data, accounts, and systems under your control. Keep passwords secure and do not share account or password information with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

3.2.2 You must maintain system-level and user-level passwords in accordance with the Password Policy.

3.2.3 You are responsible for ensuring that proprietary information remains within the control of Vandelay Industries at all times through legal or technical means. It is strictly prohibited to conduct Vandelay Industries’ business that results in the storage of proprietary information on personal or non-Vandelay Industries controlled environments, including devices maintained by a third party with whom Vandelay Industries does not have a contractual agreement. Moreover, the use of an e-mail account that is not provided by Vandelay Industries, or its customer and partners, for company business is prohibited.

3.3 Computing Assets

3.3.1 It is your responsibility to protect assigned Vandelay Industries assets, which includes the use of computer cable locks and other security devices. Laptops left at Vandelay Industries overnight must be properly locked or secured in a locked compartment. Promptly report any theft of Vandelay Industries assets to the Information Technology Services Department.

3.3.2 All PCs, PDAs, laptops, and workstations must utilize a password-protected screensaver with automatic activation set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
3.3.3 All ID cards must be removed from ID card-enabled systems when the system is not in use or is unattended.

3.3.4 Do not interfere with corporate device management or security system software, including, but not limited to, antivirus, automatic update software, pop-up blocker software, and default system administration settings.

3.3.4 Technology resources should be treated as strategic assets.

3.4 **Network Use**

You are responsible for the security and appropriate use of Vandelay Industries network resources under your control. Using Vandelay Industries resources for the following is strictly prohibited:

3.4.1 Any activities which lend themselves to the breach of company data, 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.

3.4.2 Causing a disruption of service to either Vandelay Industries or other network resources, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.

3.4.3 Introducing honeypots, honeynets, or similar technology on the Vandelay Industries network.

3.4.4 Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software. You may not operate a file-sharing or piracy system (such as Torrent sites, Pirate Bay, or similar applications). See the Vandelay Industries policy on Intellectual Property Protection for additional information on copyright restrictions.

3.4.5 Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws. See the Policy on IT Counterproliferation for additional information on export and transfer restrictions.

3.4.6 Use of the Internet or Vandelay Industries network that violates the employee code of conduct, Vandelay Industries’ policies, or local laws.

3.4.7 Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and keyloggers.

3.4.8 Port scanning or security scanning on a production network unless authorized in advance by Information Security.
3.5 **Electronic Communications**

The following is strictly prohibited:

3.5.1 Inappropriate use of communication vehicles and equipment, to supporting illegal activities, and procuring or transmitting material that violates Vandelay Industries policies against harassment or safeguarding of confidential or proprietary information.

3.5.2 Vandelay industries bans transmission or downloading of material that is discriminatory, defamatory, harassing, insulting, offensive, pornographic or obscene. This may include sending spam via e-mail, text messages, IMs, voicemail, or any other form of electronic communication.

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

3.5.4 Sending the same or similar non-business-related messages to large numbers of Vandelay Industries employees.

3.5.5 Using a company email or IP address to engage in conduct that violates Vandelay Industries policies or guidelines. Posting to a public newsgroup, bulletin board, or listserv, or a public form with a Vandelay Industries e-mail or IP address represents Vandelay Industries to the public; therefore, exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the company.

3.5.6 Use of Vandelay industries digital assets to engage in forgery will not be tolerated and there will be consequences leading up to termination of employment.

3.5.7 Social media’s Negative Use: Vandelay industries strongly encourages its employees to not engage in conduct that results in the negative use of social media.

3.5.8 Sharing of confidential information even on company provided social network is prohibited

4 **Security**

4.1.0 Use of Personal Data: During the conduction of daily business operations, it is sometimes required to share/utilize/transfer Personal Information Data (PID) among the various locations of the company located worldwide. These transfer of PID is necessary to keep the business running and to meet the business requirements but the personnel must act as stewards of Information entrusted to them.

    PID may be used as follows:

    a. To identify a Data Subject personally
b. To communicate with a Data Subject;
c. To comply with Human Resource requirements;
d. To comply with government regulations;
e. To provide associate benefits;
f. To manage the business.

4.1.1 Integrity of Personal Data. Vandelay Industries will take required steps in regards with the Personal Data and Sensitive Data:

a. Where possible, the data will be obtained directly from the Data Subject to whom the Personal Data relates;
b. The data will be obtained and processed fairly and lawfully by the Company for General Business Purposes;
c. The data will be obtained that is only relevant to General Business Purposes and will not be revealed more than what is necessary for the purpose;
d. The data will be kept up-to-date to maintain accuracy, and will not be kept more that required, while being under the control of the Company.

4.1.2 Notice: The purpose of the collection of the Personal Data will be informed to the Data subjects by Vandelay Industries. Data Subjects will not be informed by the company when the Processors are unknown about the names of the Data Subjects and Personal Data are rendered anonymous.

4.1.3 Procedure for Accessing Personal Data: Vandelay Industries, to ensure the accuracy of Personal Data will take measures, like, the company will sometimes allow reasonable access to Data Subjects to correct the Personal Data in case of any inaccurate information. The access will be allowed during normal working hours and after the proper approval of the reasonable request.

4.1.4 Security of Personal Data: Appropriate precaution measures will be adopted by Vandelay Industries in order to protect the loss, misuse, unauthorized access, disclosure, alteration and destruction of Personal Data.

5    Enforcement: Vandelay Industries reserves the right to revise, amend, or modify this AUP at any time. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Vandelay Industries:

- Suspension or revocation of account & privileges
- Disciplinary action as described in the Employees’ Code of Conduct handbook
- Civil or criminal prosecution under federal and/or state law
- Penalties under such laws may include fines, orders of restitution, and imprisonment

6    Definitions
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>honeypot, honeynet</td>
<td>Network decoys that serve to distract attackers from valuable machines on a network. The decoys provide an early warning for intrusion detection and detailed information on vulnerabilities.</td>
</tr>
<tr>
<td>Spam</td>
<td>Electronic junk mail or junk newsgroup postings. Messages that are unsolicited, unwanted, and irrelevant.</td>
</tr>
</tbody>
</table>

7 Revision History

<table>
<thead>
<tr>
<th>Date of Change</th>
<th>Responsible</th>
<th>Summary of Change</th>
</tr>
</thead>
</table>

Created referencing the generic template for acceptable use policy by FIRST.org, Inc. retrieved at: https://www.first.org/_assets/resources/guides/aup_generic.doc