Student Information Security Policy

Prospect College

January 01, 2020 to January 01, 2021

<u>Main Campus</u>
1220 19th St NW Suite 100
Washington, D.C. 20036
Tel: (202) 223-3500
Fax: (202) 223-7201
www.ProspectCollege.edu

1 USER RESPONSIBILITIES

Implementation of an effective information security policy is a team effort involving the participation and ongoing support of all employees, students, and other individuals who use Prospect College IT resources. It is the responsibility of every user to know IT security requirements and to conduct their activities accordingly. Inappropriate use exposes the Prospect College to risks including virus attacks, compromise of network systems and services, damage to reputation, and legal issues. This policy is included in the New Employee Orientation package to ensure that each new hire is familiar with Prospect College's practices regarding Information Security.

These policies do not impose restrictions that are contrary to the Prospect College's established culture of sharing, openness, trust, and integrity. However, the Prospect College is committed to protecting users and the Prospect College from illegal or damaging actions committed by individuals, either knowingly or unknowingly.

1.1 Users are accountable for their actions.

- Users are accountable for activities on Prospect College information technology resources accessed via their assigned User IDs and secret passwords. They shall not violate, aid, abet, or act in conspiracy with others to violate Prospect College policies or procedures and applicable state and federal law or regulations.
- Users shall abide by Prospect College policies and procedures pertaining to information security, confidentiality, and privacy when handling Prospect College owned or managed information.
- Users are responsible for helping to maintain the security of IT resources and protecting them from unauthorized access and malicious software, such as viruses, Trojan horses, worms, and spyware. Users shall be cautious of all file attachments and consult with the Director of Operations, who is the coordinator of the information security program, for appropriate precautions if they have questions about appropriate precautions to take.

1.2 Passwords will be protected.

- Users shall be continuously aware that all credentials (e.g., the combination of User IDs, passwords) that allow access to any Prospect College information, data, or system are explicitly the property of the Prospect College and shall only be used for conducting official business.
- Users are responsible for the protection of all passwords. If a computer password has been compromised or forgotten contact the Director of Operations to have it reset
- Users may use the same password on internal systems, network devices, or applications, but should not use their internal password for external systems, such as for accounts on an external web site, in case these web sites do not protect passwords in an acceptable manner.

1.3 Incident Response

- Users will contact the Director of Operations if they suspect a security policy violation, system intrusion, virus, or other malicious software on a Prospect College system.

1.4 Expectation of privacy

- There shall be no expectation of privacy when using Prospect College-owned information technology resources (including computers). Accordingly, users shall not have an expectation of privacy in anything that they create, place on, store, send, or receive on any Prospect College-owned information technology resources.
- Users shall respect the privacy of others when handling their personal information and shall take appropriate precautions to protect restricted information transmitted or received via computer networks and other communication devices, not limited to but including faxes, PDAs and smart phones.

1.5 Intellectual property shall be protected.

- Users shall not violate intellectual property laws (this includes copyrights, patents, trademarks, trade secrets, and/or proprietary works) and must abide by the terms and conditions associated with the use of the intellectual property. Violations can include but are not limited to illegally copying, distributing, downloading, and/or uploading information from the Internet (or any electronic source). Examples of commonly copyrighted items are audio materials, movies, videos, software, video games, pictures, and images. Free access to intellectual property does not mean it comes without protection requirements. All applicable software copyright and licensing laws must be followed.
- Users shall not repost personal communications without the author's prior consent.

1.6 Resources shall be used appropriately

- Users shall not use the Internet to stalk others, post, transmit, request, or originate any unlawful, threatening, abusive, fraudulent, hateful, defamatory, obscene, or pornographic communication, or any communication where the message, or its transmission or distribution, would constitute a criminal offense, give rise to civil liability, or otherwise violate any applicable law.
- Users shall not access or attempt to gain access to any computer account to which they are not authorized. Users shall not intercept or attempt to intercept data transmissions of any kind for which they not authorized.
- Users shall not use Prospect College IT resources for financial gain or commercial use and in no case shall the resources be used for illegal activity. Users shall not use Prospect College IT resources for using or accessing pornography, obscenity, profanity, or language offensive to another user. Users shall not use Prospect College IT resources to knowingly access material or make individual contacts or communications, which are inappropriate, and of no educational value in the context of the mission of the Prospect College.
- Users shall not play games or use software not licensed to the Prospect College on Prospect College owned resources.

1.7 E-Mail

- Users shall not send unsolicited commercial advertising or product advertisement for anything other than Prospect College official business.
- Users shall not send any type of mass mailing that does not pertain to Prospect College business or results in network spamming.

2 COMMUNICATIONS AND OPERATIONS MANAGEMENT

2.1 Anti-virus (AV) Software Provisioning and Maintenance.

- The Prospect College shall provide anti-virus software and the means to keep it up to date, without cost, to their faculty, staff, students, and other authorized users for their on-campus desktop, laptop, or server class computers. In return and as a condition of resource use, on Prospect College provided devices, all users shall have anti-virus software installed, enabled, configured for maximum protection, and up to date at all times if they intend to connect to a Prospect College network or network service at any time. If non-Prospect College-owned devices connect to the network, the device must have either Prospect College-provided or individually-owned up-to-date anti-virus software installed.
- AV software is provided “as is.” Students, faculty, staff, and others installing Prospect College-furnished anti-virus software on personal computers shall acknowledge that the anti-virus software is provided “as is” and that the Prospect College has no expressed or implied liability for its use.
- AV software configurations. Anti-virus software should be configured to scan for malicious software at start-up without user intervention. Users shall not exit from this scan nor circumvent the anti-virus configurations. The software shall scan inbound and outbound e-mail and attachments.
- Maintaining current virus definition files. Resource users shall ensure that their anti-virus software is up to date. Virus definition files shall be updated when new definition files (signatures) are released by the software vendor or announced by Prospect College OIT. Pre-set configurations to automatically or routinely update signature files shall not be changed or circumvented.
- Personnel who choose to use non-Prospect College anti-virus software in their personal PCs (that connect to the Prospect College network) shall obtain their AV software, virus signatures and virus removal files from the vendor or reputable source.

2.2 Monitoring

2.2.1 Monitoring and filtering Prospect College systems.

The Prospect College reserves the right to monitor and filter, at any time, the use of any Prospect College owned, controlled, or managed system. Monitoring will be done to ensure that systems are performing as required and that published policies, guidelines, and/or procedures are being followed.

2.2.2 Filtering inbound and outbound Internet traffic.

The Prospect College reserves the right to:

- Monitor the use of Prospect College computer systems.
- Identify unacceptable activities and/or instances of misuse, whether malicious or not.
- Collect system audit information to ensure that published policies, standards, and procedures are being followed.

3 ACCESS CONTROL

3.1 Passwords.

User Identification and Authentication are essential to ensure only authorized users obtain information. Identification is a User ID, a sequence of characters that uniquely identifies the person to whom it is assigned. User IDs typically follow an organizational convention and are quite guessable. Passwords provide Authentication that the person presenting the password is the same person that belongs to the User ID. Passwords are secret and should only be used by the personnel who create them. Users shall be held strictly accountable for any and all activities that occur as a result the use of their User ID that is authenticated by the use of their password. The key technical control to ensure authorized personnel get in and unauthorized personnel are kept out is the user-created password. This is why we place great emphasis on the creation and maintenance of strong, secret passwords.

- Passwords shall be constructed in accordance with standards and used to validate the authenticity of the person presenting the User ID.
- When passwords are used as the primary authentication mechanism, they shall be checked by the system when they are created to ensure they adhere to password construction standards.
- Any time the password is reset by someone other than the user, the operating system or database shall prompt the user to change their password before granting access. This includes initial passwords issued by network administrators for the user’s first access.
- Passwords are personal in nature and should never be written down, or given to another person.
- Good passwords are composed of alphabetic, numeric, and special characters.
- It is recommended that passwords shall be at least 8 characters in length and have 3 out of 4 of the following attributes:
    - A letter
    - A number
    - An uppercase
    - A special character