Written Information Security Programs (WISP)

Introduction

Purpose and Applicability

This Written Information Security Program or "WISP" is intended to set guidelines to safeguard the institutions confidential and restricted data stored at Washington State College of Ohio (WSCO). This program is also to ensure that the school keeps with applicable laws and compliances to insure the integrity of the aforementioned data.

Scope

This program applies to all staff, this includes full time, part time as well as contract work. This program also applies to students, alumni and, contracted third-party vendors. The data covered by this Program includes any information stored, accessed, or collected at the college or used for college operations.

Definitions

Data Classification

The College enforces necessary restrictions to protect its computing and network resources, including the revocation of use privileges for unauthorized or inappropriate use. The user is responsible for correct and sufficient use of the tools each computer system provides for maintaining the security of stored information.

Users should have no expectation of privacy when utilizing the College computer resources. While the College does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the College computing resources require the backup and caching of data and communications, the logging of activity, the

monitoring of general usage patterns, and other such activities that are necessary to provide service. The College may also specifically monitor the activity and accounts of individual users of College computing resources, including individual login sessions and communications, without notice, when:

A. It reasonably appears necessary to do so to protect the integrity, security, or functionality of the College or other computing resources or to protect the College from liability.

B. There is reasonable cause to believe that the user has violated, or is violating, this policy.

C. An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns.

D. It is otherwise required or permitted by law.

Data that WSCO is classified into three categories public, confidential and, restricted. Confidential and Restricted data both require a background check (covered in Policies for Safeguarding Restricted and

Confidential data) Public data can be view by anyone in or outside the organization. This data does not include any personal information about a student or member of WSCO or any. Confidential data that cannot be shared publicly and is only for use by the parties that require access to that data. An example of this would be grades of a student along with other contact information like phone number and personal email address. This is information cannot be shared with anyone who does have a role that can access it. Restricted Data is any personal information along with any other personal identifiable information. This is information like Social security number, home address. This level of information can only be handled by Executives, HR or the Systems Analyst in the IT Department whom are reasonable for the safe handling of this data.

Policy

Roles and Responsibilities

Washington State College of Ohio relies on the involvement and coordination of the whole IT Department. Since Washington State College of Ohio Currently Does not have a CIO and operates on a democratic agreement of the department. The responsibility of Incident(s) response falls on each member of the IT department but is coordinated by the Senior Systems Analyst and the Network and Systems Admin. It is also the responsibility of this party to report updates and findings to the VP of Organizational Effectiveness.

The Executive Director of Operations and Finance has the responsibility to report the incident and any accompanying information to the rest of management and leadership. It is up to the management and leadership teams to approve and allocate necessary resources for an incident. As well as manage any public relations that may need to be addressed including communication to the Board of Trustees, the institutions legal representatives and any applicable state entities, as required based on the nature of the incident

While specific roles have been designated for incident response, incident reporting and awareness are responsibilities shared by all staff, faculty, and students. They play a vital role in promptly reporting incidents, following incident response procedures, and participating in security awareness training programs. It is important that all individuals understand their roles and responsibilities, and actively contribute to incident response efforts. Regular training and awareness programs help ensure that everyone is prepared to fulfill their responsibilities effectively.

Organization Responsibilities

The data created by each department is the responsibility of the department and the department's dean or VP. This pertains to the safe keeping of said data in the right repositories provide to by WSCO's IT departments and not sored on private drives or devices where the IT department cannot properly protect the data.

The protection and providing storage for each department falls on WSCO's IT Department. The responsibilities of the IT department include keeping storage systems up to date with the latest security patches, installing and maintaining antivirus software and insuring the integrity of that data. The IT

department also had the responsibility of maintaining this program to provide guidance for how data should be handled.

The Human Resources department is responsible for alerting the IT department about change of employee status or termination as soon as possible. Any changes that may result in a change in employee access to college data. All parties are responsible for the safety of this data ensuring that data is only shared with appropriate parties and that access to data is based on a least privileged model.

Policies for Safeguarding Restricted and Confidential Data

Background checks are required for any parties accessing restricted or confidential data this is all employees of WSCO including part time, full time, and third-party vendors. This is to ensure the integrity of the Organization's data. This data must be stored in WSCO's databases or secure file servers and cannot be shared in any way without prior access and authorization. The data's integrity is the responsibility of the staff and the Information Technology Department.

Vendors who do not have a background check but still need access to domain connected systems that do not contain or handle Restricted or Confidential data will have access limited to only those devices. This is provided by segregating access with a limited VPN connection. All names of employees who use limited VPN access must be recorded and will be subject to investigation if a breach were to occur. If a vendor transitions to needing access to a system that transports or contains confidential or restricted information. A background check will be needed before any work is done.

In all cases vendors are only permitted on the systems that they were contracted to do maintenance on. Data from these systems should only be saved and stored on said systems owned by WSCO. Data created for or by WSCO cannot be stored on outside data stores including personal or enterprise storage solutions unless explicitly contracted to do so.

Computer system safeguards

Blocked access, Firewall

At WSCO, we take security seriously, and we use a variety of safeguards to protect our systems and data. One of our key measures is the use of a firewall, which helps us to block unauthorized traffic and shape the traffic that is allowed through. Additionally, we use GEO blocking to reduce the risk of nation-state attacks. By implementing these measures, we are able to greatly enhance the security of our systems and better safeguard the sensitive data that we store and handle.

Antivirus and monitoring

At WSCO, we understand the importance of protecting our systems and data from malware and other malicious software. To that end, we use an advanced antivirus solution that helps us to detect and prevent a wide variety of threats. This solution uses sophisticated algorithms and heuristics to identify potentially malicious activity, and is updated on a regular basis to ensure that it stays up-to-date with the latest threats. By using this advanced antivirus solution, we are able to provide an additional layer of protection for our systems and data, and ensure that our environment remains secure and reliable.

Isolated networks

At WSCO, we recognize that one of the most effective ways to protect our systems and data is to isolate our networks. We use a variety of techniques to ensure that our networks are properly segmented and isolated from one another, including the use of VLANs, firewalls, and other access control measures. By isolating our networks, we are able to limit the potential impact of a security breach, prevent unauthorized access to sensitive data, and reduce the risk of malware and other threats spreading across our environment. This approach helps us to ensure that our systems and data remain secure and that we are able to maintain the confidentiality, integrity, and availability of our resources.

Remote access

At WSCO, we take great care to ensure that remote access to sensitive data is carefully controlled and monitored. All individuals who require remote access to our systems and data are required to undergo a background check before they are granted access. This helps to ensure that only individuals with a valid business need and a clean record are able to access our resources from remote locations. Additionally, all remote traffic is closely monitored using advanced security tools and techniques. This allows us to quickly detect and respond to any suspicious activity, and helps us to ensure that our systems and data remain secure at all times. By implementing these measures, we are able to provide a high level of security for our sensitive data, even when accessed remotely.

Backups

Our robust backup system follows the industry-standard 3-2-1 method, ensuring the redundancy and availability of critical data and systems. It can instantly create virtual copies of our servers, whether on-premises or in the cloud, enabling quick recovery and minimal downtime in case of incidents.

High Availability Computing

In addition, our high availability server cluster ensures continuous availability of critical services and applications. This cluster can withstand the failure of up to two servers without causing service outages or disruptions. Through fault-tolerant technologies like load balancing and automatic failover, we maintain system reliability and uninterrupted access to essential services.

Employee Training

Constant contact and awareness

At WSCO, we understand that cybersecurity is a critical aspect of our operations. As such, we have implemented a comprehensive training program to ensure that all staff and faculty are equipped with the knowledge and skills necessary to safeguard our systems and data. Our training program covers a wide range of topics, including password security, email safety, and best practices for using technology securely. By providing this training to our employees, we are able to reduce the risk of human error and ensure that everyone is able to do their part in keeping our environment secure.

In addition to our training program, we also conduct regular phishing tests to gauge the performance of all employees. These tests simulate real-life scenarios in which employees may receive phishing emails or other malicious communications. By conducting these tests, we are able to identify areas where our employees may be more susceptible to attacks and provide targeted training to help them improve their security awareness. We also use these tests as an opportunity to provide feedback and guidance to employees who may have fallen for a phishing attempt, so that they can learn from their mistakes and improve their security practices going forward.

To ensure that our training program and phishing tests are effective, we closely monitor the performance of all employees and track key metrics such as click-through rates and completion rates for training modules. This allows us to identify trends and areas where additional training or support may be needed, and to continuously improve our overall security posture. Additionally, we provide regular feedback to employees on their performance in phishing tests and offer guidance and resources to help them improve their security awareness.

Overall, our comprehensive approach to cybersecurity training and testing helps us to ensure that our staff and faculty are equipped with the knowledge and skills necessary to protect our systems and data. By continuously monitoring and improving our program, we are able to stay ahead of evolving threats and maintain a high level of security for our environment.

Reporting Attempted or Actual Breaches of Security

At WSCO, we take the security of our systems and data very seriously, and we encourage all employees to report any attempted or actual breaches of security as soon as possible. This includes any unauthorized access or use of our systems, any loss or theft of data or devices, and any suspicious activity or communications that could indicate a security threat.

Reports of attempted or actual breaches of security should be made to our IT department or the designated security contact person. This person will then escalate the report to the appropriate authorities and take the necessary steps to investigate the incident and mitigate any potential damage. All reports should be made as soon as possible, and should include as much detail as possible about the incident, including the date and time of the incident, the nature of the incident, and any potential impacts to our systems or data.

In certain situations, additional steps may need to be taken depending on the nature and severity of the breach. This may include notifying law enforcement or regulatory authorities, engaging third-party forensic experts to conduct a detailed investigation, and taking steps to contain and recover any compromised data or systems. We also have established procedures for communicating with affected individuals and stakeholders, which may include providing them with information about the incident, offering credit monitoring or other services, and taking steps to prevent future incidents from occurring.

Overall, our approach to reporting attempted or actual breaches of security is designed to ensure that we can quickly and effectively respond to any potential threats and minimize the impact of any incidents that do occur. By encouraging all employees to report any suspicious activity or potential threats, we are able to maintain a high level of vigilance and ensure that our systems and data remain secure.

Enforcement

At WSCO, we have established a number of policies and guidelines to ensure the security and appropriate use of our systems and data. This includes our Acceptable Use Policy and our Policy Handbook, which outline the expectations and responsibilities of our employees when using our technology resources. We take the enforcement of these policies very seriously, as they are essential to maintaining a secure and reliable environment for our operations.

Our Acceptable Use Policy provides clear guidance on what activities are allowed and prohibited when using our technology resources, and sets forth the consequences for any violations. This includes disciplinary action, up to and including termination of employment, for any employee who violates the policy. Our Policy Handbook similarly outlines our expectations for employee conduct, and provides guidance on topics such as confidentiality, data privacy, and security awareness.