Washtenaw Community College

Third Party Management Policy

AN ADMINISTRATIVE INFORMATION SECURITY POLICY

PURPOSE

The purpose of this policy is to describe the information security requirements to be followed in the selection, management and monitoring of third party service providers at Washtenaw Community College. This policy also defines the information security requirements for contracts with third party service providers.

SCOPE

All engagements involving third party service providers, including vendors, consultants, and suppliers, which grant access to Washtenaw Community College information processing facilities, data or assets shall be in accordance with this policy.

ROLES & RESPONSIBILITIES

Information Security Office: Responsible to ensure compliance with this policy as a component of the College's information security program.

Management: Follows this policy for contracts with third parties. Appoints a point of contact for managing the relationship with the third party.

IT Staff: Assists sponsors and owners of the business function to be outsourced with the due diligence required.

REQUIREMENTS & PRACTICES

Prospective sponsors of outsourced services are strongly encouraged to engage the assistance of Information Technology Services (ITS) as early as possible in their project planning. It is recommended that this be considered at project inception and well in advance of establishing budget requirements.

Sponsors of outsourced services, Data Owners and owners of business functions shall exercise appropriate due diligence in the selection of the service provider, including the following considerations:

- Types of data being accessed and methods of access
- Definitions of data ownership and disposition throughout service lifecycle
- Non-disclosure and acceptable use agreements covering Washtenaw Community College assets, including facilities, systems and data
- Service provider levels of security to be provided for protecting College assets
- Service provider physical and logical controls used to restrict and limit the access to Washtenaw Community College sensitive business information
- Legal requirements to be met, such as data protection compliance requirements or regulations
- Availability and levels of service to be maintained, including in the event of a disaster
- The right to audit and review of any recent audit reports
- Clear understanding of the service provider security and incident response policy and assurance that the provider shall communicate incidents promptly
- Required screening, training, experience and other obligations of service provider staff
- Conflict and defect resolution

If the service provider provides confidential information, it is the sponsor's responsibility to ensure that any obligations of confidentiality are satisfied (see the College's *Data Classification Policy* and *Data Protection Policy*).

In situations of higher risk to protected assets, the College shall require the right to require changes to existing service provider standards or practices, if not in alignment with those of the College, and obtain access to the service provider for evaluations of its performance. In addition, the College shall require the provision of annual standardized reports including security, availability, processing integrity, confidentiality or privacy, e.g. Services Organization Control Type 2 (SOC 2) or equivalent external audit report.

Service providers that do not meet these requirements shall not be used for projects.

Arrangements involving third party access to Washtenaw Community College information processing facilities or assets shall be based on a formal contract. The contract will contain, or reference, all security requirements and the assigned responsibilities to ensure that there is no misunderstanding between the college and the third party.

Washtenaw Community College shall contractually require service providers implement appropriate security controls in accordance with Washtenaw Community College policies.

Sponsors of outsourced services, Data Owners and the owners of business functions being supported are responsible to ensure that the services provided by the service provider are monitored to confirm that they are in accordance with these policies.

The following terms shall be included in all third party contracts:

- A general policy on information security
- Asset protection, including:
    - Procedures to protect College assets, including information and software, which align with the College's *Data Classification Policy*
    - Procedures to determine whether there has been any compromise of assets, e.g., whether loss or modification of data has occurred, and requirements for reporting to the College
    - Controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during, the contract
    - Provision that the College shall remain in control of its data at all times, and in the event of a contract breach or default the

provider must agree to provide the College its data in the agreed upon format and timeline
    - Provisions regarding integrity and availability
    - Restrictions on copying and disclosing information, including the provision that College data, including system components and services, shall remain in the continental United States
    - Provision that the service provider shall perform risk assessments at least annually, but immediately following any event of significance

- Responsibilities with respect to compliance, legal and regulatory matters, including that the service provider will comply with US Federal and State legislation, commerce and export control laws in securing College data and breach response, as well as relevant or mandated standards, including:
    - Family Education Rights And Privacy Act (FERPA)
    - Department of Education Title IV Federal Student Aid Internet Gateway (SAIG) Agreement and Program Participation Agreement (PPA)
    - Higher Education Opportunity Act (HEOA)
    - Health Insurance Portability And Accountability Act (HIPAA)
    - Health Information Technology For Economic And Clinical Health Act (HITECH)
    - General Data Protection Regulation (GDPR)
    - Gramm-Leach-Bliley Act For Disclosure Of Nonpublic Personal Information (GLBA)
    - Red Flag Rules (RFR)
    - Digital Millennium Copyright Act (DMCA)
    - Payment Card Industry Data Security Standards (PCI-DSS)
    - Communications Assistance for Law Enforcement Act (CALEA)
    - Americans with Disabilities Act (ADA)
    - State of Michigan Data Breach Notification Laws
    - Other State Statutes Pertaining To Personally Identifiable

Information (PII) Protection

- Access control agreements covering:
    - Chain of custody, separation of duties, least privilege access requirements for data handling and access control
    - Permitted access methods and the control and use of unique identifiers such as user IDs and passwords
    - Lifecycle and record keeping processes for granting, maintaining and removing user access, rights and privileges
- The right to monitor, and revoke, user activity
- The right to audit contractual responsibilities, or to have those audits carried out by a mutually agreed upon third party
- Service providers reporting requirements detailing controls affecting confidentiality, integrity and availability of College information, services and systems
- A requirement that the third party is responsible for the acts of any subcontractors
- Where applicable, a description of the third party provider's contingency plans to ensure that services are maintained in the event of a disaster
- Any required physical protection controls and mechanisms to ensure that the controls are followed
- Any proprietary software, documentation and data be kept in escrow to provide the College access to these resources in the event the third party is no longer a viable entity
- An acknowledgement that the service provider is responsible for the College's information including cardholder data the service provider processes, transmits or stores
- Intellectual Property Rights (IPRs) and copyright assignment and protection of any collaborative work
- Additional potential areas of concern, as these may relate to aspects of information security, including service availability:
    - A description of each service to be made available
    - The target level of service and unacceptable level of service

- The respective liabilities of the parties to the Agreement

Accounts used by vendors for remote maintenance (including remote access accounts) shall be enabled only during the time period needed where appropriate. Remote access shall be provided in accordance with Washtenaw Community College's *Remote Access Policy*.

All passwords established and utilized by any service, account or vendor must be in accordance with the College's *Passphrase Complexity & Protection Policy*.

For third parties with access to credit card data, a list of service providers shall be maintained and the PCI compliance status of each service provider should be verified at least annually.

COMPLIANCE

This policy is a component of Washtenaw Community College information security program that is intended to comply with the PCI-DSS, FERPA, GLBA and other regulations.

EXCEPTIONS

The Chief Information Officer (CIO) or a designated appointee is authorized to make exceptions to this policy. Any requests for exceptions shall be made using the *Request for Policy Exception* form and a copy maintained by the CIO.

VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Washtenaw Community College reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

DEFINITIONS

CIA Triad: Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization.

> **Confidentiality**: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
>
> **Integrity**: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.
>
> **Availability**: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Computer: Computers are defined as workstation, desktop or laptop system, typically intended for individual or personal use.

Data: Information collected, stored, transferred or reported for any purpose, whether electronically or hard copy.

Data Owner: Data Owners are College officials having direct operational-level responsibility for the management of one or more types of data.

User: Any Washtenaw Community College faculty, staff, students or partner who has been authorized to access any College electronic information resource.

REFERENCES

Data Classification Policy

Data Protection Policy

Passphrase Complexity & Protection Policy

Remote Access Policy

Request for Policy Exception

REVISION HISTORY

Version	Description	Revision Date	Review Date	Approver
1.0	Initial version	10/11/18	-	WJO