# Security Standard for Third-Party Risk Assessment

# Purpose

[Company Name] utilizes third-party products and services to support our mission and goals. Third-party relationships carry inherent and residual risks that must be considered as part of our due care and diligence. The Third-Party Information Security Risk Management Policy contains the requirements for how [Company Name] will conduct our third-party information security due diligence.

# Audience

This policy applies to all individuals who engage with a third-party on behalf of [Company Name].

# Policy

Departments should use the Information Security Third-Party standards to assess all third-party IT service arrangements. Examples include:

* Web hosting
* Application Development
* Database Management
* Network Monitoring
* Web content development
* Data Backup
* System Maintenance
* Offsite Storage

Again, the process is recommended for all third-party IT service relationships; however, the process is mandatory where Confidential/High Risk data is accessed remotely, transmitted, or stored offsite. In these instances, the Information Security Third-Party Assessment Survey must be reviewed by the Information Security Team.

# Procedure

The following domains shall be reviewed as a part of [Company Name]'s third party information security assessment process:

### Governance, Risk and Compliance

Third party vendors shall comply with [Company Name]’s Third-Party Information Security Risk Management Policy

### Human Resources Management

Third party vendors shall comply with [Company Name]’s Identity and Access Management Policy

### Incident Management

Third party vendors shall comply with [Company Name]’s Incident Management Policy

### Third Party Management

Third party vendors shall require any third party subcontractors or vendors to comply with the standards outlined in this policy.

### Access Management

Third party vendors shall comply with [Company Name]’s Identity and Access Management Policy

### Password Security

Third party vendors shall comply with [Company Name]’s Password Protection Policy

### Remote Access

Third party vendors shall comply with [Company Name]’s Remote Access Policy

### Network Security

Third party vendors shall comply with [Company Name]’s Network Security Policy

### Threat/Vulnerability Management

Third party vendors shall comply with [Company Name]’s Data Breach Response Policy

### Change Management/Software Development

Third party vendors shall comply with [Company Name]’s Change Control Policy

### Asset Management

Third party vendors shall comply with [Company Name]’s Asset Management Policy

### Data Handling/Disposal

Third party vendors shall comply with [Company Name]’s Data Classification and Management Policy and Data Destruction and Sanitization Policy

### Physical Security

Third party vendors shall comply with [Company Name]’s Physical Security Policy and Technology Equipment Disposal Policy

# Waivers

Waivers from certain and specific policy provisions may be sought following the [Company Name] Waiver Process. There are no exceptions to any provisions noted in this policy until and unless a waiver has been granted.

# Enforcement

This Third-Party Information Security Risk Management Policy supplements and compliments all other related information security policies, it does not supersede any such policy or vice versa. Where there are any perceived or unintended conflicts between [Company Name] policies, they must be brought to the attention of [Company Name] for immediate reconciliation.

Personnel found to have violated any provision of this policy may be subject to sanctions up to and including removal of access rights, termination of employment, termination of contract(s), and/or related civil or criminal penalties.

# Version History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Modified Date** | **Approved Date** | **Approved By** | **Reason/Comments** |
| 1.0.0 | September, 2020 | September, 2020 |  | Document Origination |
|  |  |  |  |  |
|  |  |  |  |  |