MORAINE PARK TECHNICAL COLLEGE

CYBER SECURITY AND HECVAT

MPTC Solicitation Identification Commodity/Service: _____

MPTC Solicitation Identification Number: _____

Moraine Park Technical College (MPTC) recognizes that it is exposed to both internal and external risks related to cyber security. Since technological growth is not static, new risks are created regularly. Accordingly, MPTC has adopted various safeguards to protect data assets and infrastructure. As a vendor of MPTC, we have a reasonable expectation that our chosen vendor will comply with basic cyber security safeguards including, but not limited to, the following as applicable.

1. Account Security. Access to MPTC technology requires robust account practices that include strong passwords and multi-factor authentication.
    - Vendor access to the MPTC network will be provided based on the principle of least privilege and role-based access controls.
    - Vendor accounts will not be shared between multiple people. Each user should have their own account.
    - Vendor accounts will be secured with long, complex passwords meeting minimal complexity requirements imposed by MPTC.
    - Vendor accounts will be secured with multi-factor authentication (MFA).
2. End Point Protection. Access to MPTC data and technology should be limited to those devices that are patched regularly and protected with anti-malware software.
    - Vendor access to the MPTC network will be provided via MPTC's Virtual Desktop Infrastructure.
    - MPTC virtual desktops are comprised of a Windows desktop and a suite of applications tailored to the specific use case needs.
    - No MPTC software assets will be installed on vendor devices without formal Information Technology approval.
    - Vendor owned software assets are not allowed to be installed on MPTC devices without formal Information Technology approval.
    - Vendor owned devices accessing the MPTC network must be protected by up-to-date anti-malware software.
3. Securely Manage Data. The handling of MPTC data should include best practices for both storing and transmission. Depending on sensitivity, this may include encryption or other safeguards to prevent unauthorized access to that data.
    - Vendor work products should be stored in the MPTC network ecosystem or remain accessible by MPTC with appropriate access controls.

MORAINE PARK TECHNICAL COLLEGE

CYBER SECURITY AND HECVAT

- Vendor downloading of MPTC data assets away from the MPTC network ecosystem is strongly discouraged.
- Depending on sensitivity, appropriate safeguards such as data encryption should be employed for MPTC data in transit and at rest.

4. Regulatory Compliance. Depending on the classification of data being handled, there may be various regulatory compliance safeguards that must be adhered to by both MPTC and third-party vendors. It is critical that regulatory compliance is maintained when applicable.
   - Vendors working with MPTC data controlled by regulatory compliance entities must follow the practices and guidelines imposed by those requirements.

5. Due Diligence. As a vendor of MPTC, it is expected that there be a pattern of resiliency, security, and observance of best practices when interfacing with MPTC data and technology.
   - Vendors may be asked to provide additional information about their Company's security practices, including completing a Vendor Security Questionnaire.
   - Vendors are expected to comply with MPTC's Acceptable Use of Computing Resources Policy.

6. HECVAT. As applicable, vendor may submit their HECVAT assessment for the College's consideration to confirm the information, data, and cyber security policies are in place to protect the Colleges' sensitive institutional information and personal identifiable information (PII).

7. PHYSICAL ACCESS to MPTC buildings and facilities is managed by the MPTC's Security Manager. All access needs to buildings or facilities will be coordinated and assigned at the sole discretion of the MPTC Security Manger team.