This Trend Micro Customer Notification (this “Notification”) provides a summary of data security and protection practices that are implemented in the Trend Micro Cloud Service. The terms and conditions for using Service Offerings are governed by Terms of Services for Trend Micro Cloud Services.

1. Responsibilities
   1.1 Your Accounts. Please refer to Acceptable Use section in 2.8 of Terms of Services for Trend Micro Cloud Services.

   1.2 Your Content. Please refer to Responsibility for Company Data section in 4.1.1 of Terms of Services for Trend Micro Cloud Services.

   1.3 Your Security and Backup. You are responsible for properly configuring and using the Service Offerings and otherwise taking appropriate action to secure, protect and backup your accounts and Your Content in a manner that will provide appropriate security and protection, which might include use of encryption to protect Your Content from unauthorized access and routinely archiving Your Content.

   1.4 Log-In Credentials and Account Keys. Please refer to Authentication Credentials section in 3.2 of Terms of Services for Trend Micro Cloud Services.

   1.5 End Users. You will be deemed to have taken any action that you permit, assist or facilitate any person or entity to take related to this Notification, Your Content or use of the Service Offerings. We do not provide any support or services to End Users unless we have a separate agreement with you or an End User obligating us to provide such support or services.

2. Changes
   2.1 To the Services. We may change or discontinue any of the Services from time to time. Please refer to Trend Micro End-of-Life Policy.

   2.2 To the Service Level Agreements. We may change, discontinue or add Service Level Agreements from time to time.

3. Term; Termination
   3.1 Termination.
      (a) Termination for Convenience. You may terminate this Notification for any reason by providing us notice and closing your account for all Services for which
we provide an account closing mechanism. We may terminate this Notification for any reason by providing you at least 30 days advance notice.

(b) Termination for Cause.
   (i) By Either Party. Either party may terminate this Notification for cause if the other party is in material breach of this Notification and the material breach remains uncured for a period of 30 days from receipt of notice by the other party. No later than the Termination Date, you will close your account.

   (ii) By Us. We may also terminate this Notification immediately upon notice to you (A) for cause if we have the right to suspend, (B) if our relationship with a third-party partner who provides software or other technology we use to provide the Service Offerings expires, terminates or requires us to change the way we provide the software or other technology as part of the Services, or (C) in order to comply with the law or requests of governmental entities.

3.2 Effect of Termination.
(a) Generally. Upon the Termination Date:
   (i) except as provided in Section 3.2(b), all your rights under this Notification immediately terminate;
   (ii) you will immediately return or, if instructed by us, destroy all Trend Micro Content in your possession

(b) Post-Termination. Unless we terminate your use of the Service Offerings pursuant to Section 3.1(b), during the 30 days following the Termination Date:
   (i) we will not take any actions to remove from the Trend Micro systems any of Your Content as a result of the termination; and
   (ii) we will allow you to retrieve Your Content from the Services only if you have paid all amounts due under this Notification.

For any use of the Services after the Termination Date, the terms of this Notification will apply and you will pay the applicable fees.

4. Service Functionality
   Please refer to on-line document of each Trend Micro service.

5. Security and Data Privacy
   5.1 Secret Authentication Information.
   You use mechanism provided by Trend Micro in section 5.2 to protect encryption keys and secrets like certificates, connection strings, and passwords in the cloud.

   5.2 Cryptography.
Trend Micro uses an industry standard and community-vetted encryption implementation for data in transit and data at rest to protect confidential and sensitive information from unauthorized disclosure and modification.

5.3 Backup Capabilities.
Trend Micro performs backup regularly to ensure and maintain the integrity and availability of information.

5.4 Secure Development Procedures and Practices
Relevant measures are implemented in accordance with ISO 27001, ISO 27017 and compliable regulations, please refer to the official site. For further details, please go to https://www.trendmicro.com/en_ca/about/legal/product-certifications.html?modal=s2a-btn-foundations-read-more-3c901e.

5.5 Information Security Measures and Capabilities
Relevant measures are implemented in accordance with ISO 27001, ISO 27017 and compliable regulations.

Trend Micro Information Security Organization performs following processes to ensure the appropriate information security controls are established to prevent information security threats and attacks.

- **Vulnerability Management**
  This process includes identifying, classifying, remediating and mitigating technical vulnerabilities on all compute instances. The security scanning is performed on a periodic basis or by request if needed.

- **Security Monitoring and Security Incident Management**
  Trend Micro established the security management procedure to ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken and information security incidents are managed in a consistent and effective approach. The procedures also include the requests for potential digital evidence or other information within the Trend Micro cloud service environment.

- **Continuous Risk Evaluation**
  Periodic reviews of the security of its network infrastructure, information security program is conducted.
5.6 Protection of Records.

Please refer to Personal Data Protection section 4.2 of Terms of Services for Trend Micro Cloud Services.

6. Others

6.1 Information of Critical Operations and Procedures.
Trend Micro has identified and documented critical operations components required to maintain the availability of our system and recover service in the event of outage. For more information please refer to on-line product information.

6.2 Service Monitoring Capabilities.
Trend Micro 24x7 cloud service operation team collects and correlates logs, and analyzes correlated events in periodical basis through engineering ways. The response process involves all stakeholders to ensure service quality and take appropriate responses.

The time synchronization mechanism of Trend Micro’s systems should be addressed in any appropriate method.

6.3 Technical Vulnerabilities.
Relevant measures are implemented in accordance with ISO 27001, ISO 27017 and compliant regulations, please refer to the official site. For further details, please go to https://success.trendmicro.com/vulnerability-response#current-claims.

6.4 Legal Jurisdictions and Compliance.
For further details, Please refer to Venue/Jurisdiction section of Terms of Services for Trend Micro Cloud Services.