Office 365

Office 365 Security & Compliance

Data Security & Privacy

- Encryption at rest protects customer data on Microsoft's servers.
  - BitLocker disk encryption.
  - Per-file encryption with a unique per-file key.
- Encryption in transit with SSL/TLS protects customer data transmitted to/from Microsoft.
- Threat management, security monitoring, and file/data integrity prevents or detects any tampering of data.
- No data access or mining for advertising purposes.
- Commitment to student privacy – http://studentprivacypledge.org
- Data hosted in-region (e.g. U.S. Data Centers for U.S. customers).
- Customer controls for tailoring security & privacy to customer needs and requirements.
  - eDiscovery[1]
  - In-Place Hold[2]
  - Rights Management[2]
  - Data Loss Prevention (DLP)[2]
  - S/MIME & Office 365 Message Encryption[2]
- Customer data isolation.

Compliance Standards[3]

- HIPAA compliance through physical, administrative, and technical safeguards. Microsoft will sign a HIPAA BAA with any customer.
- FISMA compliance.
- ISO 27001 security standards compliance.
- U.S. – EU Safe Harbor Framework.
- FERPA compliance.
- CIPA/COPPA compliance.
- SSAE 16 SOC 1 Type I and Type II, and SOC 2 Type II.
- Gramm-Leach-Bliley Act (GLBA) compliance.

Service Continuity

- Geo-redundant, in-region data centers.
- Multiple copies of customer data within and between data centers.

Resources

- Office 365 Trust Center: http://trustoffice365.com/
- Office 365 Security White Paper: http://go.microsoft.com/fwlink/p/?LinkId=401240
- Student Privacy Pledge: http://studentprivacypledge.org

[1] eDiscovery for email is included in all Office 365 E plans. Office 365 E3 & E4 plans also include the eDiscovery center for discovery across documents and email.
[2] Some features may require an Office 365 E3 or equivalent subscription.
[3] Regulatory compliance FAQ: http://go.microsoft.com/fwlink/p/?LinkId=335734.

Microsoft