INFO-TECH SYSTEMS INTEGRATORS PTY LTD
Suite 65, Level 4, 330 Wattle St,
Ultimo NSW 2007
Tel: (61) 2 7201 9808
www.info-tech.com.au

SECURITY WHITE PAPER

Data Center

Microsoft Azure is engaged as a cloud service provider, where Info-Tech hosted and stored its Cloud HR Software and Database. The data center is located at the Australia East (Australia). Microsoft Azure employs multi-layered security across the physical data Center, infrastructure, and operations. Data centers managed by Microsoft have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the data center floor.

Data Encryption

We encrypt all data in transit between customers and Info-Tech using TLS 1.2 or higher protocols. For data at rest, we are using 256-bit Advanced Encryption Standard (AES). Info-Tech's web-based applications are also encrypted end-to-end with an SSL Certificate by default. Info-Tech has also implemented extra layers of security on the cloud application – for example, Multi Factor Authentication, and secure HTTPS to ensure data transiting to Azure are encrypted and secured.

Security Threat and Vulnerability Management

Info-Tech uses Microsoft Defender Advance Threat Protection to help enterprise networks prevent, detect, investigate, and respond to threats. Also, internal, and external (Third-party assessment) Vulnerability Assessment and Penetration Test (VAPT) is being performed for all Applications, API, and Servers as mentioned below frequency to identify flaws to protect critical data and ensure that our networks and systems are not exposed to cyberattacks as well as to ensure security weaknesses are being discovered and remediated.

VAPT - Mode	Frequency
Internal	Once in three months
External	Once in a year

User Authentication

We provide users with standard access to Info-Tech Cloud HR software through a login username and password. As an extra layer of security, Info-Tech also offers Two-Factor Authentication (2FA) for user login. If 2FA login is enabled, the user will be required to enter a One-Time Password (OTP) that has been generated and sent to the user's smartphone. We recommend customers to use 2FA to reduce risk and mitigate cyber

threats. We have provided access logs screen, where customer can view their employees' login date & time with IP address.

Password Policy

Info-Tech has implemented a global password policy and the user should meet the following password criteria to create and access the account.

- Password Should be 8 to 20 characters long.
- Password contains a mixture of lower-case, upper-case, numbers and special characters [$,&,@,#,^, etc..].
- Password Max- Age - 60/90 Days (Customized)
- Forced password change when first time login.
- Account gets locked out after 5 wrong attempts.

Customer's Control

Info-Tech customer has the flexibility to add employees/users into their account within the number of head count that have subscribed. The person with the super-admin role has the control over who has access and what they are able to do. Our Software Support Specialist will not access to customer's confidential information unless request initiated for assistance via the ticketing system or telephone call. We are doing everything to protect customer's data. Please see our **Terms of Service** and **Privacy Policy** for further information.

Customer Database Backup & Retention

We do have regular 7-day database backup and server backup of zone redundance at Info-Tech.

Also, we hold the data in the customer's account as long as the customer chooses to use Info-Tech Cloud HR Software. Once the account is terminated, customer data will be deleted from the active database after 30 days from the termination date. We will give customers a prior notice via email before the permanent deletion of your database. Complete back up will be deleted after 7 days from the active database deletion.

Information Security Awareness Training

All employees will receive security awareness training throughout their career with Info-Tech. During onboarding, employees will receive a Data Protection Management Programme communication email, which encourages employees to adopt and promote good data protection practices in our organization. Employees will also be given access to the internal security policies. Additionally, there will also be weekly email that to constantly remind employees of security issues and the best practices that they should follow to ensure safe handling and storage of data.

INFO-TECH SYSTEMS INTEGRATORS PTY LTD
Suite 65, Level 4, 330 Wattle St,
Ultimo NSW 2007
Tel: (61) 2 7201 9808
www.info-tech.com.au

Disposal of Physical Devices

We have an authorized vendor to carry out the disposal of unusable physical devices (e.g. laptop, tablet, hard disk). Any information contained inside the devices is formatted before disposal. The hard drives will be degaussed which destroys remnant magnetic fields on magnetic components, heads and domains on hard drives by exposing them to a strong magnetic field. This guarantees that any information is no longer retrievable and the hard drive that's been degaussed can never be used again.

Physical and Environmental Security

Info-Tech's office premise is monitored 24/7 through surveillance cameras, which capture the images of those entering the premises. Multiple layers of security controls are implemented to protect the access to and within our environment, including firewalls, intrusion protection systems and network segregation. Cisco Meraki firewall is implemented to monitor and control incoming and out-going network traffic based on the firewall rules defined by the organisation. Preventive maintenance for all physical devices such as window updates, antivirus updates, antivirus scan, capacity review and UPS battery health check will be done as per the established schedule. If any information processing system (hardware, software and data) is to be taken off-site, relocating or transferring, proper authorization will be obtained. For assets sent for repairs, all data are to be backup and information are to be erased from any hard disk and then sent for repair or discard. Necessary records for removal/ disposal of such assets are maintained and recorded.

Security Breach

We have a rigorous incident management process for security events that may affect the confidentiality of data. We have a dedicated emergency response team to take over the responsibility for managing security incidents. In the event of a potential data breach, we will carry out assessment of the data breach expeditiously within 30 days. If the data breach is assessed to be likely to result in significant harm or impact to the individuals whom the personal data relates, we will notify the customer no later than 24 hours after establishing that the data breach is likely to result in significant harm or impact to the individuals, or of a significant scale (i.e. data breach involves personal data of 500 or more individuals).

We are committed to keeping your data safe and secure, by using best practices to protect our system and your data. Should you have any concerns with regards to our Network & Security and Data Protection practices, please contact our Security Team at security@info-tech.com.sg or Data Protection Officer at dpo@info-tech.com.sg

INFO-TECH SYSTEMS INTEGRATORS PTY LTD
Suite 65, Level 4, 330 Wattle St,
Ultimo NSW 2007
Tel: (61) 2 7201 9808
www.info-tech.com.au

Global Cyber Protection by CHUBB - Cyber Enterprise Risk Management

In today's connected environment, cyber security is a widespread concern. With this in mind, we have added cyber insurance to our businesses around the globe as an additional layer of security while also gives our stakeholders peace of mind and confidence to move forward with Info-Tech. Cyber protection can also assist in the timely remediation of cyberattacks and security incidents.

SECURITY WHITE PAPER LAST UPDATED: 27th SEPTEMBER 2023