INFO-TECH SYSTEMS INTEGRATORS PTE LTD
30 Kallang Place #07-14 Singapore 339159
Tel: (65) 6297 3398 Fax: (65) 6297 7008
www.info-tech.com.sg
Registration No: 200711480W

Your HR Matters On The Go!

SECURITY WHITE PAPER

OUR CERTIFICATIONS

ISO 27001:2013 Certified Information Security Management Systems (International Standard)

SS 584:2015 Certified Multi-Tier Cloud Computing Security Assurance (Singapore Standard)

Info-Tech certified with the Data Protection Trustmark (DPTM) under IMDA

Info-Tech is certified as compliant with ISMS ISO 27001: 2013 and Multi-Tier Cloud Security Management System of Singapore (MTCS) - most widely known information security management standard used by organizations to keep data assets secure. Info-Tech achieved these certifications by developing and implementing a robust security management program to keep our customers data safe. On top of that, Info-Tech has also been awarded with the Data Protection Trustmark (DPTM) certification by @Infocomm Media Development Authority (IMDA). What does this mean? It means that customers and employees can rest assured that the personal data under Info-Tech's care is responsibly managed and safeguarded.

Data Center

Microsoft Azure is engaged as a cloud service provider where Info-Tech host and stored its Cloud HR Software and Database. The data center is located at the South East Region (Singapore). Microsoft Azure employs multi-layered security across physical data centers, 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 that in transit between customer and Info-Tech using 256-bit Advanced Encryption Standard (AES), whereas Info-Tech's web-based applications are encrypted end-to-end with SSL by default. Info-Tech has also implemented extra layers of security on the cloud application – for example 2 Factor Authentication, secure HTTPS to ensure data transit to Azure are encrypted and secured.

INFO-TECH SYSTEMS INTEGRATORS PTE LTD
30 Kallang Place #07-14 Singapore 339159
Tel: (65) 6297 3398 Fax: (65) 6297 7008
www.info-tech.com.sg
Registration No: 200711480W

Your HR Matters On The Go!

Security Threat and Vulnerability Management

Info-Tech uses Microsoft Defender Advance Threat Protection to help enterprise network prevent, detect, investigate and respond to threats. Vulnerability assessment will be conducted on a yearly basis, on Info-Tech's IT systems and network, to identify flaws to protect critical data and ensure that our

networks and systems aren't exposed to cyberattacks. Penetration test will be conducted on a quarterly basis, on Info-Tech's IT infrastructure and applications to ensure security weaknesses are being discovered and remediated as soon as possible.

User Authentication

We provide users with a 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, user will be required to enter a One-Time Password (OTP) that have been generated and sent to the users' smartphone. We recommend customer 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.

Customers' 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 ticketing system or telephone call. We are doing everything to protect customer's data. Please see our **Terms of Service** and **Data Protection Policy** for further information.

Customer Database

We hold the data in customers account as long as customer choose 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 customer a prior notice via email before the permanent deletion of your database.

Information Security Awareness Training

All employees will receive security awareness training throughout their career with Info-Tech. During onboarding, employees will receive 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 PTE LTD
30 Kallang Place #07-14 Singapore 339159
Tel: (65) 6297 3398 Fax: (65) 6297 7008
www.info-tech.com.sg
Registration No: 200711480W

Your HR Matters On The Go!

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 24X7 through surveillance cameras which capture the images of those entering the premises. Multiple layers of security controls 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 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 asset 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 incident. 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 72 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 concern with regards to our Network & Security and Data Protection practices, please contact our Data Protection Officer at dpo@info-tech.com.sg

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.