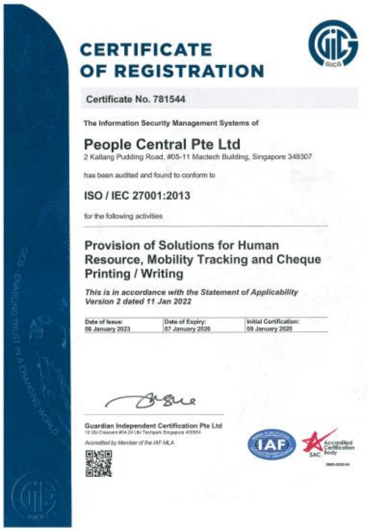
PEOPLE
CENTRAL

PeopleCentral Pte Ltd
2 Kallang Pudding Road
#05-11 Mactech Building
Singapore-349307
www.peoplecentral.co

SECURITY WHITE PAPER

OUR CERTIFICATIONS



CERTIFICATE
OF REGISTRATION

Certificate No. 781544

The Information Security Management Systems of

People Central Pte Ltd
2 Kallang Pudding Road, #05-11 Mactech Building, Singapore 349307

has been audited and found to conform to

ISO / IEC 27001:2013

for the following activities

Provision of Solutions for Human Resource, Mobility Tracking and Cheque Printing / Writing

This is in accordance with the Statement of Applicability Version 2 dated 11 Jan 2022

Date of Issue:	Date of Expiry:	Initial Certification:
08 January 2023	07 January 2026	09 January 2020

Guardian Independent Certification Pte Ltd
10 Ubi Crescent #04-24 Ubi Techpark Singapore 408564

Accredited by Member of the IAF MLA

GICG
GICG · ENABLING TRUST IN A CHANGING WORLD
IAF
SAC Accredited Certification Body

1. Customer Control and Confidentiality

Customers retain control over their accounts, managing user access based on subscribed headcounts. Super-admin roles regulate access privileges to specific Modules and functionalities. Our Software Support person accesses customer information solely upon request through formal channels, such as a ticketing system or phone call, prioritizing data protection and security

We continuously refine access control protocols to grant users the necessary access without compromising data security.

2. User Access and Authentication

Access to People Central's HRMS software is granted through standard login credentials. As an added layer of security, Two-Factor Authentication (2FA) is available, requiring a One-Time Password (OTP) generated and sent to the user's smartphone. Encouraging the use of 2FA helps mitigate cyber threats. . Access and Audit logs provide transparency, allowing customers to monitor their employees' login details.

We periodically review and update our authentication policies in alignment with evolving security standards and best practices.

3. Data Encryption Standards

All data transmitted between customers and People Central Cloud environment is encrypted using TLS 1.2 or higher protocols. For data storage, we employ 256-bit Advanced Encryption Standard (AES). Our web-based applications utilize end-to-end encryption with SSL Certificates as a default security measure. Additionally, our cloud application employs supplementary security layers, including Multi-Factor Authentication and secure HTTPS, to fortify the encryption and security of data transmitted to Azure & AWS.
Our commitment to data security extends to robust encryption practices. TLS protocols and AES encryption standards ensure secure data transmission and storage.

We continuously assess encryption technologies and practices to adopt the most robust and up-to-date encryption standards, ensuring the highest level of data protection.

4. Data Center Infrastructure

People Central engages Microsoft Azure & Amazon Web Services (AWS) as its cloud service provider, hosting and storing the PeopleCentral HRMS Software and Database in a Tier-4 data center situated in the South-East Region (Singapore). Microsoft Azure & Amazon Web Services (AWS) implements a multi-layered security approach across its physical data centers, infrastructure, and operations. These data centers feature extensive protective measures, encompassing access control at various levels: facility perimeter, building perimeter, internal building access, and within the data center itself. The Tier-4 data center, housed within the South-East Region (Singapore), offers optimal security through its multi-tiered access control mechanisms. Microsoft Azure & Amazon Web Services (AWS) maintains rigorous protocols across physical and operational aspects, ensuring comprehensive protection for the stored data. Each layer of defense, from perimeter security to internal access, undergoes stringent scrutiny and control measures to safeguard against unauthorized access or breaches.

5. Physical and Environmental Security Measures

Our office premises are under 24/7 surveillance through surveillance cameras. We implement multiple layers of controls, including firewalls and network segregation, ensuring robust access controls and network security. Routine preventive maintenance, including updates for software, antivirus etc. is conducted according to established schedules, and stringent protocols are followed for off-site information processing or asset repairs.

We maintain comprehensive security measures and protocols to ensure the physical and environmental safety.

6. Security Threat and Vulnerability Management

People Central leverages '**Microsoft Defender Advanced Threat Protection'** and '**Amazon GuardDuty'** to fortify our network against potential threats. Additionally, We conduct both internal and external Vulnerability Assessment and Penetration Tests (VAPT) at specified intervals for all Applications, APIs, and Servers. These assessments occur with a frequency of '**Once Every Three Months Internally'** and '**Once A Year Externally'** to identify and address vulnerabilities that may compromise critical data security.
Our approach to threat management involves proactive measures like Microsoft Defender Advanced Threat Protection and 'Amazon GuardDuty' respectively and regular Vulnerability Assessment and Penetration Testing. These evaluations, conducted periodically, serve to identify and rectify vulnerabilities, shielding our networks and systems from potential cyber threats or vulnerabilities.

7. Incident Management and Security Breach Protocol

We possess a well-defined incident management process and an emergency response team to take over the responsibility for managing security incidents.
In the event of a potential data breach, We will assess the data breach and ensure that notification protocols are implemented to notify impacted parties within 24 hours of determining that the data breach is likely to cause substantial harm or impact to an individual or on a large scale.

Our commitment to prompt breach assessment and notification aligns with our dedication to data security and customer trust.

8. Secure Information Handling and Transfers

Any off-site transfer or relocation of information processing systems requires proper authorization. Assets sent for repair undergo data backup and subsequent erasure before being serviced or discarded. Comprehensive records of asset removal/disposal are diligently maintained.

9. Information Security Training

All employees undergo security awareness training, emphasizing data protection practices. Onboarding includes a Data Protection Management Programme, granting access to internal security policies. Regular communication reinforces security protocols and best practices.

Our ongoing training initiatives ensure employees remain updated on evolving security threats and best practices.

10. Secure Disposal of Physical Devices

Authorized vendors handle the disposal of unusable physical devices after formatting information contained within. Degaussing processes are employed on hard drives to render data irretrievable, ensuring complete data security before disposal.
Our disposal procedures prioritize data security by employing rigorous formatting and degaussing measures on unusable physical devices, preventing any potential data retrieval.

We strictly adhere to industry-standard protocols for secure data disposal to prevent any potential data breaches.

11.Customer Database Backup & Retention Policy

We maintain regular 7-day database backups and implement server redundancy measures. Data remains in customers' accounts as long as they utilize People Central HRMS Software. Upon account termination, data is securely deleted from the active database after a 30-day grace period, with prior notice to the customer.

We strictly adhere to established timelines for data retention and deletion to honor privacy commitments.

12. Commitment to Data Security

We remain dedicated to upholding stringent security practices and employing best-in-class measures to protect both our systems and your valuable data.
The extended details provided further underscore the depth of security measures implemented by People Central. Clear protocols for incident management and data breach notifications ensure transparency and proactive engagement in addressing potential security issues. This reiteration of commitment assures customers of People Central's unwavering dedication to safeguarding their data.