SECURITY WHITE PAPER

AutoCount e-Invoice Platform

Version 1.0

AUTO COUNT SDN BHD

Last Modified 04/10/2024

Change History

Version	Date	Prepared by	Description
1.0	04/10/2024	Jae Sen	Initial Release

1. Overview

AutoCount e-Invoice Platform (hereinafter AIP) is a dedicated server hosted to streamline any connection, data transmission, e-Invoice submission and validation from AutoCount solutions to IRBM's MyInvois Portal via IRBM's provided APIs. AutoCount solutions that are currently connecting to AIP for e-Invoice purpose are not other than:

1. AutoCount Accounting 2.2
2. AutoCount Point of Sales 5.2, Retail Edition
3. AutoCount Point of Sales 5.2, F&B Edition
4. AutoCount Point of Sales 5.2, Optical Edition
5. AutoCount Cloud Accounting
6. AutoCount OneSales, POS Edition
7. AutoCount OneSales, Palm POS

2. Data Hosting and Security

AIP utilizes Huawei Cloud as its cloud service provider for hosting, storing and running functional requirements related to e-Invoice submission and validation. This data centre is situated in Southeast Asia (Singapore) with the location generally safe from natural disasters and other risks. Huawei also implemented access control, enforcing minimum access possible to any personnel who needs to enter or exit data centers. Besides, video surveillance system and infrared system monitoring is installed to monitor every cabinet unit to ensure that all data servers are physically safe. Intrusion detection system with alarm is also available 24/7 to detect and monitor any security events, allowing the quickest respond from onsite security to attend to the event.

Some of Huawei's notable certifications related to security and cybersecurity:

- ISO 22301
- ISO 27001
- SOC 1 Type II, SOC 2 Type II and SOC 3
- PCI DSS Level 1
- DJCP Level 4
- CSA STAR Gold

**List of certifications can be found at Huawei Cloud official website: https://www.huaweicloud.com/intl/en-us/securecenter/compliance.html (Website is accessible as 4th October 2024)*

3. Data Collection

The purpose of AIP is to aid in the implementation of Malaysia e-Invoice, integrating with our own AutoCount solutions to ensure the best user experience for our clients. Some of the data that will be collected are not other than:

1. Company or individual details required by Malaysia e-Invoice.

2. Transactional data used for submission which includes Invoice, Credit Note, Debit Note, Consolidated Invoice and Self-billed Invoice data. Details of data are as per required by Malaysia e-Invoice.

4. Data Privacy

Protecting client's data privacy is fundamental to our operations. Robust framework and security best practice is applied to ensure client's personal data and business information remains confidential and is used only when intended. Our data strategy includes:

- **Data Access Control:** We enforce strict access controls and permissions to ensure that only authorized personnel can access these data. We also practice allowing the minimum number of personnel to access these data ensuring the lowest risk possible of data exposure.
- **Data Minimization:** Adhering to the principle of data minimization, we only collect data required to deliver our services.
- **Transparency:** We inform clients about what data and how the data is collected, used and protected though clear privacy policies.
- **User Rights:** Clients have all the rights on their data. We provide clients way to access their respective data to update or correct inaccuracies. Additional email validation is required as extra security step to ensure the action is taken by the right person. Clients also have the rights to exercise data deletion whenever applicable.
- **Data Sharing Consent:** If any data is required to be shared to one or more party for convenience or functional purpose, we will always ask consent from the clients, ensuring that all parties had agreed on the sharing of data. We will also state clearly what data will be shared to ensure clients are being informed to avoid dispute in future.

5. Data Encryption

Encryption is one of the most important part of data protection strategies. We utilize advanced encryption technologies to ensure that any data exchange risk is minimized and safe.

- **In-Transit Encryption:** Communication and data exchange between AIP and mentioned AutoCount solutions are encrypted using HTTPS with Transport Layer Security 1.2. This ensures that data exchanged over the internet is always protected from eavesdropping and tampering.
- **At-Rest Encryption:** Our database uses AES-256 encryption, a strong standard for encrypting data at rest. This is to ensure that data is safeguard against any unauthorized access.

6. Information Security

Our information security encompasses a range of security strategy ranging from technical to organizational measures to safeguard your data.

- **ISO 27001 Compliance:** We adhere to ISO 27001, an internationally recognized standard for information security management. This certification ensures that we always comply and follow the best practices for managing and protecting data. Refer appendix for certification.

- **Close Monitoring and Incident Response:** We had special assigned specialist to closely monitor AIP to identify any potential threats or suspicious activities.
- **Employee Training:** We conduct regular training for employees on data protection and security best practices. This is to create a culture of understanding the importance of security and awareness to ensure everyone is well knowledge and aware on handling sensitive information
- **Backup and Recovery:** We perform routine backup on AIP's data to ensure data can be restored in any case of unexpected incident. Currently we are using RDS service in Huawei Cloud for database backup. This service comes with 2 types of automatic backups, first is differential backup every 5 mins and second is a daily full backup. With such practice, we can ensure that even if any unexpected incident happens, continuity of services can be resume in a very short period due to the minimum data differences. Additionally, we also have our own full backup daily that will be synced to our own storage server.
- **Third Party Risk Assessment:** We engage third party to perform penetration test on our server and services. We are currently at the engagement phase for this part. Results will be updated after the full test had been done.

7. Retention Policy

We practice data retention to not keep obsolete data in our server for long periods. As per current practice, we will purge of transactional data after 90 days. Within the 90 days, these transactional data is serves for validation purpose in any case that cross checking against actual submission or results is required. As for company and individual details, we held no responsibility to edit or remove these data and clients will need to take full responsibility to delete these data permanently if required.

8. Appendix

No.	Compliance	Certification
1.	ISO/IEC 27001:2022	Refer to file: IS 770012 – 001.pdf Refer to file: IS 770013 – 001.pdf
2.	Penetration Test by Third Party	Pending