

VPN-Authentication mechanisms and compliance

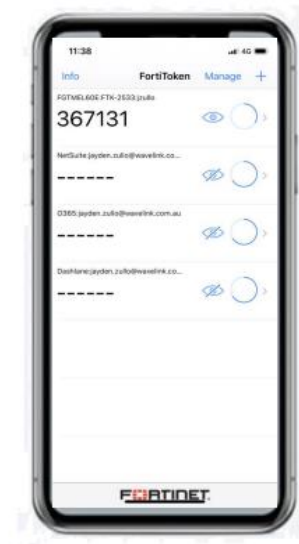
(Classification and Handling -Safeguarding Sensitive and Confidential Information)

Proprietary Notice: This document contains proprietary information that is confidential in BPO Convergence Company. Disclosure of this document in full or in part, may result in material damage to BPO Convergence. Written permission must be obtained from BPO Convergence prior to the disclosure of this document to a third party.

At Swiggy, we prioritize robust security measures to safeguard our digital environment and ensure seamless operations. All associates must adhere to the following access guidelines:

1. VPN Access

- **Fortified Security:** VPN access is protected by FortiToken-based two-factor authentication (2FA).
- **Mobile Integration:** Associates are required to use the FortiToken app on their mobile devices for secure token generation.
- **ID-Based Access:** VPN IDs are exclusively generated using employee IDs, ensuring strict alignment with organizational protocols.



2. Email Access

- **Advanced Authentication:** Microsoft Authenticator is implemented for 2FA during email login to provide an extra layer of security.
- **Vigilance:** Any unusual email activity is monitored, and access violations are promptly addressed.

3. General Security Measures

- **Device Security:** Associates must safeguard their devices used for accessing company resources. Lost or compromised devices must be reported immediately.
- **Compliance:** Regular training on cybersecurity and adherence to IT policies is mandatory.

Commitment to Security

Compliance with this policy is essential for protecting Swiggy's digital assets. Any deviations may result in access restrictions and further actions as deemed necessary.