BUNDL TECHNOLOGIES Pvt. Ltd

IT Infrastructure

Remote Access Management Policy

Title of work:	Bundl Technologies	Year of Creation of Work:	2019
Category:	Internal	Full Date of Publication:	4 Nov 2019
Version:	1.0	Total Pages:	8
Description:	Describes about Remote access to BTPL Infrastructure in structured manner	Reviewed by:	General Manager - InfoSec
Author:	Compliance Team	Approved by:	Director - IT

REFERENCES: Requirement of ISO/IEC 27001:2013, SSAE 16, SOC 1, SOC2.

TABLE OF CONTENTS

1. Objective:

The objective of this policy is to provide controlled remote access into the BTPL's corporate & Cloud network. The policy is designed to safeguard from unauthorized use of BTPL resources.

2. Scope:

This policy applies to all employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs accessing BTPL's resources remotely.

3. Policy:

Remote access to BTPL's corporate & Cloud resources from public network shall be allowed only after successful identification and authentication of users

BTPL Usage VPN as service to provide remote access feature to all respective employees/contractors/vendors/franchise to access internal applications

Approved employees of BTPL and authorized third parties (customers, vendors, etc.) may utilize the benefits of remote connection services

Employees shall be responsible for provided remote access(VPN) privileges to ensure that unauthorized users are not allowed access to internal networks

Employees shall exercise caution while using mobile devices and connecting to BTPL network remotely from public places, meeting rooms and other unprotected areas

Remote access logs shall be maintained for 90 days

Access denial logs on remote access service shall be monitored for taking preventive & corrective actions

Remote Access Services (VPN) must be controlled using MFA (Multi Factor Authentication) and Password mechanism or shall be authenticated by the Active Directory. Also, User Authentication for establishing remote access services (VPN) session shall be encrypted

When actively connected to the BTPL corporate network via authorized endpoint devices, all traffic shall flow through secured communication channels such as SSL or IPSEC tunnel

Dual (split) tunneling is NOT permitted; only one network connection is allowed.

VPN services will be set up and managed by IT Infrastructure Team

Remote access to BTPL resources by third party must have written approval from Information Security Manager

All computers connected to internal networks via remote access services (VPN) must use updated anti-virus software as per the BTPL standard.

In case of system is not updated with latest Antivirus, OS patches, VPN service shall not be allowed to connect to Swiggy Network

VPN users will be automatically disconnected from 's network after 15 minutes of inactivity. Pings or other artificial network processes are not to be used to keep the connection open.

VPN is strictly allowed only on company owned devices

Role Based Access:

- IAM team shall have defined roles for respective departments in the organization
- IAM shall create different groups as per organizational units and different departments specific requirements
- User shall be added to respective group as per the request and requirement of the request.
- Access to respective groups shall be given post approval from respective authorized personnel

4. Policy Compliance

4.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to,

Internal and external audits,

periodic walk-throughs,

Security tool reports & Dashboards,

Review & Reporting.

4.2 Exceptions

Any exception to the policy must be approved by the Infosec head & CTO in advance.

4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

References

BTPL_IT Security policy

BTPL_Code of Business conduct

BTPL_Password policy

BTPL_Laptop Policy

5.0 Disclaimer

IT Compliance Team of Bundl Technologies reserves all rights and is the exclusive owner of all intellectual property rights over this information security policy and procedure document. This information security policy and procedure document shall not, either in part or in full, be reproduced, published, copied, displayed, distributed, transferred, stored into any media (such as floppy diskettes, hard disks, USB Drives, Pen Drives, Memory Cards, CDS, DVD's), and/or captured or transmitted through by any means (electronic, digital, mechanical, photocopying, recordings, video and film or photographs and otherwise) by any person without prior written consent from the Head of IT.

6.0 Acronyms Used

Acronym	Expanded Form	Acronym	Expanded Form
OS	Operating system	VPN	Virtual Private Network
IT Head	Heading BTPL IT	Swiggy	BTPL
HR Head	Person Heading BTPL Human Resource	BTPL	Bundl Technologies Pvt. Ltd. (Swiggy)

END