SERVICE PACKAGE: SL0027

ANTI-VIRUS SECURITY

Consulting Cloud Preview

IT SERVICE PRODUCT OVERVIEW 4
Reference # 4
Name 4
Description 4
Inclusions 4
Exclusions 5
SUPPORTED BUSINESS OUTCOMES 5
Business Importance Level (BIL) 5
Customer outcomes 5
Vital Business Functions (VBF) 5
Business drivers 5
AVAILABILITY 7
Service hours 7
Exceptions 7
Usage peak periods 7
Critical business cycles 7
Other critical assets 7
Archiving 7
Availability targets 7
UNAVAILABILITY 8
Unavailability exclusions 8
Business impact of unavailability 8
Change & Release windows 8
Change & Release restrictions 8
SERVICE CONTINUITY 8
Disaster recovery 8
SUPPORT REQUIREMENTS 9
Customer support plans 9
3rd Party Support 9
Support details 9
PRICING 9
Price description 9
Price drivers 10

Consulting Cloud Preview

Limitations 10
INCLUDED COMPONENT SERVICES 10
RESPONSIBILITIES 10
Customer 10
CUSTOMER 10
End User 10
SERVICE MANAGEMENT DETAILS [Refer: Customer Services Handbook] 11
Customer Service Owner(s) 11
CUSTOMER Business Service 11
Owner (s) 11
Change control 11
Dates 11
SERVICE LEVEL TARGETS 12
Availability 12
Reliability 12
Maintainability 12
Support 12
Performance 13
Capacity 13
Management Information 13
Service Requests 13
Continuity 13

Consulting Cloud Preview

Note: The audience for this IT Service Product is the CUSTOMER executive who hold the budget and makes purchasing decisions (the IT Service Product buyer).

1.0	IT SERVICE PRODUCT OVERVIEW	
1.1	**Reference #**	SL0027
1.2	**Name**	Anti-virus Security
1.3	**Description**	This service covers the activities required to prevent unauthorized electronic access to Customer infrastructure. Electronic access to the infrastructure is protected by a firewall that is configured to block all communication ports not required by the hosted software. To prevent the spread of Viruses and Trojans, email is scanned for malicious content, and suspect messages are quarantined before reaching the rest of the Customer network.
1.4	**Inclusions**	♦ Firewall configuration. ♦ Anti-virus software. ♦ Data encryptors for secure communications between two sites. ♦ Scanning and quarantine of email (malware and spam related). ♦ Patching of infrastructure for security reasons (though this is also covered in software and security patching service). ♦ Physical access to the infrastructure. ♦ Protection of Desktop PCs and Laptops is covered by Desktop SOE virus scanning software. ♦ Assessing software (e.g. website forms, Lotus Notes) for security vulnerabilities. Communication: Refer to **Customer Service Handbook (CSH)** for establishment communication protocol between CUSTOMER and Customer.

Consulting Cloud Preview