# PROVISION OF AZURE PLATFORM INFRASTRUCTURE FACILITIES MANAGEMENT

## Technical Solution

# Document Confidentiality Statement

The information in this document is confidential to the company to whom it is addressed and should be used for that purpose only. It may not be reproduced in whole, or in part, nor may any of the information contained therein be disclosed for any purpose outside the addressee's company without the prior written consent of Xtremax Pte. Ltd. The addressee's company shall have the right to duplicate and use the data for its own internal evaluation. A recipient may not solicit, directly or indirectly (whether through an agent or otherwise) the participation of another institution or person without the prior approval of the directors of Xtremax Pte. Ltd.

# Table of Contents

# Server Management

Xtremax provides Server Management services which will include the following:

1. System Administration
2. Active Directory, Web Server and Application Server Administration
3. Database Server Administration
4. Archival, Backup and Recovery Administration
5. Server Security Administration
6. Performance and Fault Management
7. Network Server Management
8. Report Requirements

## System Administration

Here are several System Administration tasks will be performed by Xtremax:

a. User administration including administration of user accounts and granting access to files and directories;
b. Managing and maintaining system utilities and scripts;
c. System configuration management including modifying system settings, drive mappings;
d. Managing and monitoring batch jobs;
e. Database Server administration including administration of Database backup, restoration, log reviews and data patch requests.
f. Server security and vulnerability patch management;
g. Server and application performance monitoring and alerts
h. System security administration such as:
    i. Monitor and perform SSL certification/software licence renewal for the systems per chargeable service requests
    ii. Manage the encryption/decryption keys for the server;
    iii. Management of system logs

There is also Server Maintenance as part of System Administration. Within it, Xtremax will also obtain any approval before performing maintenance on the servers. And as defined by our client at the start of the contract, Xtremax will send out a notification to all involved parties. For server

maintenance at a specific time, Xtremax will schedule and inform it first. As per the client's instructions, Xtremax will perform all start-up and shutdown of servers.

## Active Directory, Web Server and Application Server Administration

Xtremax will perform the following administration activities for Active Directory, Web Server and Application Server:

a. Administer and support the configurations of Domain Controller configurations, connection to new Servers and support creation of required domain accounts;
b. Manage application servers, services, application pools, network communications,
c. Handle database connectivity and messaging;
d. Manage connections to web servers, databases and other systems;
e. Perform fault and performance management;
f. Respond to monitoring alerts and perform first-level troubleshooting when required;
g. Provide access to the application team for troubleshooting when required;
h. Perform reviews of accounts and logs.

## Database Server Administration

Xtremax will perform the following administration activities for database server:

a. Manage and monitor the database storage, database space utilisation, table extents and growth, and alert or report to the customer on performance or capacity issues
b. Setup and manage the user accounts, access rights, privileges, roles and profiles;
c. Plan and perform database backup and recovery;
d. Plan and schedule regular database housekeeping and maintenance activities necessary to keep the database in a healthy state and at optimal performance;
e. Manage scripts and database object deployment;
f. Perform fault and performance monitoring;
g. Respond to monitoring alerts and perform first-level troubleshooting when required;
h. Perform database patch management
i. Provide access to the application team for troubleshooting when required;
j. Perform joined reviews of exception logs.

## Archival, Backup and Recovery Administration

The scope of the archival, backup and recovery administration will include the backup and recovery of the following:

a. Operating systems;
b. Application;
c. Database;
d. User and applications data; and
e. System configuration.

Xtremax will perform the archival, backup and recovery activities in accordance such as:

a. Backup and restore jobs;
b. Support the recovery of server and storage.

## Server Security Administration

Xtremax shall ensure that the Servers are kept up to date with security patches. The management of Security Patches is elaborated as follows:

### Security Patch Management

On a regular basis, Xtremax monitors information proactively and releases new security patches on a timely basis. Xtremax receives notifications of advisories from customer Representatives as and when it is made available. Then, Xtremax will implement the patches/advisories if it is applicable.

Regularly, Xtremax tests the patches and confirms that they are free of malicious codes. Every update of the software will be installed, before deploying in a production environment. Security patches will be implemented according to the timeframe stipulated below:

Timeline for patch evaluation, testing, packing (if any) and availability:

Table 2. Timeline for each type of Patch Evaluation

| Type of Patch (Evaluation) According to Security Risk Classification | Timeline |
|---|---|
| Emergency | Within **twelve (12)** hours |
| High | Within **three (3)** days |

| | |
|---|---|
| Medium / Low | Within **two (2)** weeks |
| Non-security related patches (e.g., Function Patches or Service Packs) | **Three (3)** months |

Timeline for patch deployment, testing, packing (if any) and availability:

Table 3. Timeline for each type of Patch Deployment

| Type of Patch (Deployment) According to Security Risk Classification | Timeline |
|---|---|
| Emergency | Within **twelve (12)** hours |
| High | Within **four (4)** days |
| Medium / Low | Within **twenty-five (25)** days |
| Non-security related patches (e.g., Function Patches or Service Packs) | **Three (3)** months |

Xtremax will establish a vulnerability and security patch management process to ensure thorough tracking of security vulnerabilities for all the assets used for the System:

a. Track vulnerability alerts and assess their applicability monthly or when issued by GITSIR
b. Perform criticality review and testing
c. Conduct change management review
d. Plan for contingency or roll back
e. Implement patches

## Performance and Fault Management

a. Xtremax will provide performance and fault management for the Cloud Environment.
b. Xtremax will provide 24x7 monitoring of the Cloud Environment servers to ascertain the general health of the servers and to detect faults or errors.
c. Xtremax will monitor the following system parameters:
    i. CPU utilisation
    ii. Memory utilisation
    iii. Disk space utilisation, including the amount of hard disk space left
    iv. Errors generated in the system logs

d. Xtremax will install monitoring agents to the servers if required by the proposed monitoring solution.
e. Xtremax will work with the customer to define the monitoring thresholds for the system.
f. Xtremax will respond to the alerts in accordance with the incident management process.
g. Xtremax will perform monitoring, collection of performance statistics and provide exception reports. When required by the customer, Xtremax will provide the data gathered from the monitoring to be used for the investigation of the root cause of system-related issues.

## Network Server Management

Xtremax shall perform any or all of the following system administration tasks related to network servers that are being managed in the AZURE environment:

a. Manage virtual private cloud network
b. Manage and maintain DNS records using cloud-native tools
c. Manage Load Balancer (e.g., NLB, ALB)
d. Deploy, manage and maintain content delivery network
e. Implement virtual private cloud peering, establishing private links with virtual private cloud endpoints, Elastic Network Interface (ENI), Elastic IP, Internet Gateway, IP block reservation, Security Group, Network Access Control List (NACL), Virtual Networks, web application firewall and enhanced networking.

## Report Requirements

Xtremax will provide the following monthly server availability and utilisation reports to the customer and the format of the report will be subject to the customer's approval. The server utilisation report will include:

a. CPU utilisation
b. Memory utilisation
c. Storage utilisation

# Security Management

Xtremax makes sure that the security of all servers is not compromised. By performing virus scanning using anti-virus software on all servers with the latest updated virus definitions files. Then, Xtremax notifies the customer on all security violation attempts and/or security breaches on the server. Xtremax will analyse the severity and propose appropriate solutions and take immediate action to curb all security violations and intrusions upon detection.

Later on, Xtremax changed the root and administrator passwords based on customer policy. Last, Xtremax will put in place and maintain up-to-date anti-virus software with the latest updated virus definitions files on all servers.

# Incident & Problem Management

## Severity Level Definition

Table 4. Severity Level Definition

| Severity Level | Description |
|---|---|
| 1 | • Unavailability of AZURE Environment under management that halts time critical System and affects majority (50% or more) of users<br>• Creates public inconvenience/alarm/chaos and is time-critical<br>• Security Breaches of Cloud Environment<br>• Malicious security attacks<br>• Virus attacks disrupting cloud services<br>• Unauthorised access to the Cloud Environment<br>• Leakage of data, information, System password or user credential |
| 2 | • Unavailability of AZURE Environment under management but not time critical and affects not more than 30% of the users<br>• Malicious security or virus attacks in some impact on the agency's ability to perform its function<br>• Access restrictions are inadvertently changed or removed, exposing the data affecting one but resulting in no adverse impact on the business operation of the agency. |
| 3 | • Unavailability of AZURE Environment under management but not time critical and affects only a few users and existing alternatives are available. |

| | |
|---|---|
| | • Report of unsuccessful attempt to violate information security (e.g. scans and probes, spoofing of emails, spam/scam emails, application/device whitelisting violation) |

## Incident Management

1. Xtremax will submit an incident report for all Severity Level 1 incidents, describing the problem, root cause, corrective actions and preventive measures. The interim or draft incident report will be submitted to the customer within twenty-four (24) hours upon the occurrence of the incident and a final report within seventy-two (72) hours. The incident report will only be closed by the customer upon full resolution of the root cause.
2. Xtremax will alert the customer of service disruptions and security incidents with Severity Level 1 immediately via SMS and/or email within FIFTEEN (15) minutes after the incident has been detected.
3. For Severity Level 1, the alert will describe the incident encountered and advise the customer on the possible resolution time and/or follow up action to be undertaken by the customer. Subsequent updates will be provided every ONE (1) hour via email and the service portal (if any) until services are restored to normal.
4. Xtremax will provide a daily summary to the customer of service disruptions and security incidents (for Level 1) for the day and the status of open incidents from previous days. The daily summary will be sent via email at the end of the day. There will be no notification if there are no incidents reported or pending incidents from previous days.
5. The incident resolution time begins upon either communication of the incident to Xtremax's service desk or customer, or detection of the incident by Xtremax's personnel or monitoring Systems.
6. Xtremax will be responsible to ensure that the customer is kept updated on the latest status of the reported defects or problems in accordance with the timeline stipulated in the table below.

Table 5: Response Time

| Severity Level | Expected Service Resumption or Response Time |
|---|---|
| | (A) First FIFTEEN (15) minutes from the occurrence of the incident: Establish the cause of incident and resolve the incident. If the incident cannot be resolved within the time limit, the Contractor will immediately inform customer and escalate the incident to |

| | |
|---|---|
| | the respective product vendors to troubleshoot the incident concurrently. Contingency or bypass methods should be used if incident occurs during support hour to quickly resume the normal service if possible.<br><br>(B) Within TWO (2) hours from the occurrence of the incident: The incident must be resolved within TWO (2) hours from the point of incident. |
| 2 | (A) First FIFTEEN (15) minutes from the occurrence of the incident: Establish the cause of incident and resolve the incident. If the incident cannot be resolved within the time limit, the Contractor will immediately inform customer and escalate the incident to the respective product vendors to trouble shoot the incident concurrently. Contingency or bypass methods should be used if incident occurs during support hour to quickly resume the normal service if possible.<br><br>(B) Within FOUR (4) hours from the occurrence of the incident. The incident must be resolved within FOUR (4) hours from the point of incident. |
| 3 | (A) First FIFTEEN (15) minutes from the occurrence of the incident: Establish the cause of incident and resolve the incident. If the incident cannot be resolved within the time limit, the Contractor must immediately inform customer and escalate the incident to the respective product vendors to trouble shoot the incident concurrently. Contingency or bypass methods should be used if incident occurs during office hour to quickly resume the normal service if possible.<br><br>(B) Resolve incident within THREE (3) working days. |

# Change Management

Change management will be classified into **THREE (3) types**, namely:

1. **Standard** – Changes that do not have any direct impact on users and frequently repeated without substantial differences,
2. **Emergency** – Any changes that are intended to repair an error in a system or services that are negatively impacting users and does not qualify as a Standard Change,
3. **Normal** – Changes that do not have any direct impact on users and are not frequent.

The following are categories of changes according to their purposes:

a. Deployment of new Government on Commercial Cloud System (AZURES) services or any supporting AZURES services
b. Enhancement of existing AZURES
c. Enhancement to mitigate IT Security Risk
d. Resolution of Incident or Problem

e. Validation of a AZURES component or services, or functionality of a AZURES component or service
f. Change of a AZURES component, service, or Configuration Item (CI) operational status/configuration
g. Retirement of a AZURES component or service, or functionality of AZURES component or service
h. Fulfillment of an agency's business requirement

In terms of the fulfillment of Service Request (SR), the service level shall be defined as follows:

a. Automated SR shall be within 4 hours from the time SR approved
b. Manual SR shall be within 2 working days from the time the SR approved. E.g. extraction of logs, installation service, installation of SSL certificates, etc.

# Capacity Management

Xtremax will define and implement monitoring indicators for all AZURES components, services and CIs of the Master Contract to monitor their capacity utilisation and performance. These monitoring indicators shall be agreed to by GovTech Representatives.

In terms of capacity utilisation, Xtremax will adopt the definitions of "warning" and "critical" thresholds as 60% and 80% utilisation respectively, unless otherwise specified or agreed to by GovTech Representative.

# System Availability

The following definitions shall apply for System Availability:

- The System Availability Level shall be 99.5%
- The System Availability is calculated on a monthly basis
- "Planned Total Service Uptime" refers to the scheduled operating hours of the respective System and services for which the System is available for on-line access
- "Planned Total Service Uptime" shall be computed based on the product of 24 hours per day and the number of calendar days per month

- “Scheduled Service Downtime” refers to the unavailability of the service for the month due to scheduled maintenance approved by customer in writing
- “Unscheduled Service Downtime” refers to unscheduled or ad-hoc service maintenance not approved by customer or service failure caused by hardware, operating System, software, abuse, mismanagement or human error, and
- System Availability shall be determined according to the following formula:
    - Availability = Actual Total Service Uptime / Planned Total Service Uptime
    - Actual Total Service Uptime = Planned Total Service Uptime – Unscheduled Service Downtime
    - Planned Total Service Uptime (in hours) = 24 hours per day x Number of Calendar days in a month– Scheduled Service Downtime

# Service Levels Performance Reporting

Xtremax will submit a monthly service report to the CUSTOMER and will ensure the report include minimally the following:

1. Executive summary of all service level achievements against defined targets, applicable liquidated damages, and major events and issues that happened in the reporting period.
2. Service level performance of the service desk, and statistics relating to service desk operations.
3. Service level performance of incidents resolution, and statistics relating to Incidents.
4. Availability and capacity utilisation for the scope under Server management.
5. Patch compliance status, and details on all non-compliance.
6. Details of all outstanding problems, and all problems resolved or closed within the reporting month.
7. Details of all changes approved or implemented in the reporting month, and their status and results.
8. Details of major operational activities that were performed (e.g., technology refresh, major software release).
9. Forward schedule of activities (e.g., include preventive System or service maintenance, technology refresh and patch deployment).
10. Data pertaining to The Contractor’s staff members’ access rights to CUSTOMER’s systems.
11. Quarterly Vulnerability Assessment Reports on the Servers managed.