Contract TRXX1
Operation and Maintenance of CCTV1
Monthly Security Report for February 2024

Table of Content   **Page**

ANNEX LIST

Annex A	Data centre access review report
Annex B	System administrator account and access rights review report
Annex C	Contractor's org chart
Annex D	System administrator add/remove request report
Annex E	End users access review report
Annex F	Vulnerability assessment report
Annex G	Penetration testing report
Annex H	Annual calendar of scheduled O&M activities
Annex I	Audit logs review report
Annex J	Log review for privileged users
Annex K	Virus definition updates report
Annex L	Vulnerability management report
Annex M	IT Inventory report
Annex N	Patch management report
Annex O	Incident report
Annex P	Backup and restoration report
Annex Q	Storage media disposal report
Annex R	Change request report
Annex S1-5	System performance reports
Annex T	Risk assessment report
Annex U	System fitness assessment report

1. **Executive Summary**

There is no incident reported during the reporting month.

The system, database and network performance were healthy during the reporting month.

There was no security alert notification and no security incident for the reporting month.

2. **Accomplishments for this Period**

2.1 Tech Refresh

2.1.1 BOS Servers are undergoing Tech Refresh due to EOL/EOS.
Target to complete by May 2024.

3. **Planned Activities for the Coming Period**

3.1 Tech Refresh

3.1.1 Video Content Analytics Servers Load Testing in Progress
3.1.2 Operator Training and familiarisation in progress.
3.1.3 Undergoing Bug Fixes and features validation
3.1.4 To be completed by End May 24

4. **User Access Review**

4.1 Data Centre Access Review

4.1.1 Physical access to data centre for the reporting month has been reviewed. Please refer Annex A.

4.2 System Administrators Access Review

4.2.1 The account and access rights of the following system administrators and service accounts for the reporting month has been reviewed. Please refer to Annex B.

a. Application administrators
b. Database administrators
c. Middleware administrators – Not Applicable
d. OS administrators
e. Remote administrators' access
f. Firewall administrators
g. Network administrators
h. Service accounts
** Application administrators refer to application software administrators, e.g. SAP admin

4.2.2   For accounts held by contractors, this has been reviewed against the org chart with names and roles & responsibilities. Refer to Annex C for the org chart.

4.2.3   The system administrator requests (added/removed) for the reporting month has been reviewed. Refer to Annex D.

4.2.4   For personnel with remote administration rights, the records of such authorised personnel, purpose of access, and validity period of personnel's authorisation has been reviewed. The validity period of personnel authorisation is shorter than one calendar year. Personnel whose access rights are expiring have been reminded to submit renewal applications Please refer to Annex B.

4.3   End Users Access Review (To be provided by users)

4.3.1   The account and access rights of the end users for the reporting month has been reviewed. The review covers the followings and inactivity/suspended accounts. Please refer to Annex E. (To be provided by users)

    a.   Staff resignation or retirement
    b.   Termination
    c.   Transfer to another agency – Not Applicable
    d.   Role changes within the agency
    e.   Extended leave
    f.   Extended party user resignation / redeployment

4.4   Others Access Review

4.4.1   All accounts after 90 calendar days of inactivity with the exception of accounts that belong to the members of public were reviewed and disabled.

4.4.2   All accounts on the last day of their authorised use were disabled. These accounts shall be removed and have their access rights revoked within the next five working days.

4.4.3   Unnecessary accounts were disabled, and default credentials were changed.

5.   Security Management

5.1   Vulnerability Assessment Reports

5.1.1   VA was conducted on 15 Feb 2024, no vulnerability found. The next VA is scheduled for June 2024.

5.1.2   Any applicable findings arising from the VA report will be schedule for closure as follows:

Type/ Criticality of patch	Deployment upon availability of patch (System)	Deployment upon availability of patch (Endpoint Devices)
Emergency	24 hours	24 hours
Critical/High	60 calendar days	30 calendar days
Medium/ Low	90 calendar days	60 calendar days

    a.   OS – refer to the table above.
    b.   Network - refer to the table above.
    c.   Application - refer to the table above.

5.2 Penetration Testing

5.2.1 VA was conducted on 15 Feb 2024, no vulnerability found. The next PT is scheduled for June 2024.

5.2.2 The penetration tests are conducted by independent and competent personnel with industry recognised certifications and using formalised methodologies. Refer to Annex G.

5.2.3 Any applicable findings arising from the PT will be schedule for closure as follows:

Type/ Criticality of patch	Deployment upon availability of patch (System)	Deployment upon availability of patch (Endpoint Devices)
Emergency	24 hours	24 hours
Critical/High	60 calendar days	30 calendar days
Medium/ Low	90 calendar days	60 calendar days

5.3 Log Review

5.3.1 The audit and security related logs for the reporting month has been reviewed. The review frequency shall be monthly. Refer to Annex I.

- a. Window OS logs
- b. Database logs
- c. Middleware logs – Not Applicable
- d. Firewall logs
- e. IDS logs
- f. Router/switch logs
- g. Application logs

S/No	Audit Log Review Description	Opened	Closed	Pending	Exception	Remarks
1.	Windows OS Audit	0	0	0	0	
2.	IDS log	0	0	0	0	
4.	McAfee Firewall Log	0	0	0	0	
5.	Fortinet Firewall Log	0	0	0	0	
6.	DB Log	0	0	0	0	

5.3.2 Log review for privileged users for the reporting month has been conducted. Refer to Annex J.

- a. OS administrators
- b. Application privileged users
- c. Database administrators
- d. Middleware administrators - Not Applicable
- e. Firewall administrators.
- f. IDS administrators
- g. Router/switch administrators

5.4 Virus Definition Updates

5.4.1 Virus definitions are updated as at Dec 2022. All servers are scanned and remediated, where applicable. Refer to Annex K.

5.5 <u>Vulnerability Management</u>

5.5.1 No Security alert notifications were received.

6. IT Inventory Management

6.1 The IT inventory for the reporting month has been updated and reviewed. Refer to Annex M. The inventory list includes:

    a. Hardware (including any asset with data storage capabilities)
    b. Software (including application software, system software and mobile software)
    c. SSL certificate (including the expiry date)
    d. EOL/EOS dates
    e. DNS record
    f. Portable storage media

The inventory list shall include system owner information.

6.2 Physically check for the presence of the assets during the month and account for those assets that are missing.

6.3 Conducted annual audit checks and accounting such as inventory checks on portable storage media issued and the assignment of write access to the authorized users of all issued portable storage media.

7. Patch Management

7.1 The security alerts, applicability and implementation status have been reviewed. Refer to Annex N.

    a. Window OS
    b. Database
    c. Middleware – Not Applicable
    d. Firewall
    e. IDS
    f. Router/switch
    g. Application

8. Incident Management

8.1 The incident reports for the reporting month have been reviewed. Refer to Annex O.

9. Backup and Media Management

9.1 The backup and restoration reports for the reporting month have been reviewed. Refer to Annex P.

9.2 The storage media disposal for the reporting month has been reviewed. Refer to Annex Q.

10.   Change Management

10.1   The system change requests for the reporting month have been reviewed. Refer to Annex R.

a.   Window OS
b.   Database
c.   Middleware – Not Applicable
d.   Firewall
e.   IDS
f.   Router/switch
g.   Application

11.   System Performance and Analysis

11.1   System Availability

11.1.1   Please refer to Annex S-1. All the servers achieved 100% availability.

11.2   Windows System Resource Utilisation

11.2.1   Refer to Annex S-2. The CPU, memory and disk utilisation were overall healthy.

11.3   Database System Resource Utilisation

11.3.1   Refer to Annex S-3. This was overall healthy with the average CPU utilisation around 40% to 55% for the reporting month.

11.4   Network Resource Utilisation

11.4.1   Refer to Annex S-4. The link bandwidth consumption was overall healthy for the monitored links.

12.   IT Governance

12.1   Risk assessment for the year has been conducted. The risks identified from the risk assessment has been reviewed. Refer to Annex T.

13.   Annual O&M Activities

13.1   The annual calendar of scheduled O&M activities has been reviewed. Refer to Annex H for details.

13.2   The annual calendar includes the following activities:

a. VA & PT schedule

b. Briefing on ICT policy, standards, and security

c. Project management meeting schedule

d. Conduct risk assessment / self-assessment / audit

e. Review and update Exit Plan

f. Disaster Recovery / Business Continuity exercise

Annex A
Data Centre Access Review Report

S/N	Name	Role/ Designation	Reviewed	Purpose of Access	Date of Review
1	Phxxxxx Chxx	Backend Manager	Yes	Backend Manager	3 Apr 2024

Annex B
System Administrator Account and Access Rights Review Report

S/N	Name	Account Role	Account ID	Reviewed	Date of Review
1	Phxxxxx Chxx	Application administrators	BOSADMIN	Yes	3 Apr 2024
2	Phxxxxx Chxx	Database administrators	BOSADMIN	Yes	3 Apr 2024
3	Phxxxxx Chxx	OS administrators	BOSADMIN	Yes	3 Apr 2024
4	Phxxxxx Chxx	Remote administrators' access	BOSADMIN	Yes	4 Apr 2024
5	Phxxxxx Chxx	Firewall administrators	BOSADMIN	Yes	4 Apr 2024
6	Phxxxxx Chxx	Network administrators	BOSADMIN	Yes	4 Apr 2024

Annex C
Contractor's Org Chart

```
                    ┌─────────────────────┐
                    │  Hexxx Txxx         │
                    │                     │
                    │  Project Director   │
                    └──────────┬──────────┘
                               │
                               ▼
                    ┌─────────────────────┐
                    │  Mxxx Axxx          │
                    │                     │
                    │  Project Manager/   │
                    │  Maintenance Manager│
                    └──────────┬──────────┘
             ┌─────────────────┼──────────────────┐
             ▼                 │                  ▼
   ┌──────────────────┐        │       ┌──────────────────┐
   │ Phxxxxx Chxx     │        │       │ Rxxxxxx Yxxx     │
   │                  │        │       │                  │
   │ Backend Manager  │        │       │ BOS Manager      │
   └────────┬─────────┘        │       └────────┬─────────┘
            ▼                  ▼                ▼
   ┌──────────────┐   ┌──────────────┐   ┌──────────────┐
   │ Backend      │   │ Maintenance  │   │ BOS Team     │
   │ Team         │   │ Team         │   │              │
   └──────────────┘   └──────────────┘   └──────────────┘
```

```
                    ┌─────────────────────┐
                    │   Rxxxxxx Yxxx      │
                    │   BOS Manager       │
                    └─────────────────────┘
                              │
                              │──────────────────┐
                              │                  ▼
                              │        ┌─────────────────────┐
                              │        │   Sxxxx Kxxx        │
                              │        │   BOS Supervisor    │
                              │        └─────────────────────┘
                              │
              ┌───────────────┼───────────────┐
              ▼                               ▼
   ┌─────────────────────┐         ┌─────────────────────┐
   │   Axxx Pxxx         │         │   Lxx Lx Yxx        │
   │   BOS Operator      │         │   BOS Operator      │
   └─────────────────────┘         └─────────────────────┘
              │                               │
              ▼                               ▼
   ┌─────────────────────┐         ┌─────────────────────┐
   │   Yxxx Cxxx Yx      │         │   Txx Txx Mxx       │
   │   BOS Operator      │         │   BOS Operator      │
   └─────────────────────┘         └─────────────────────┘
```
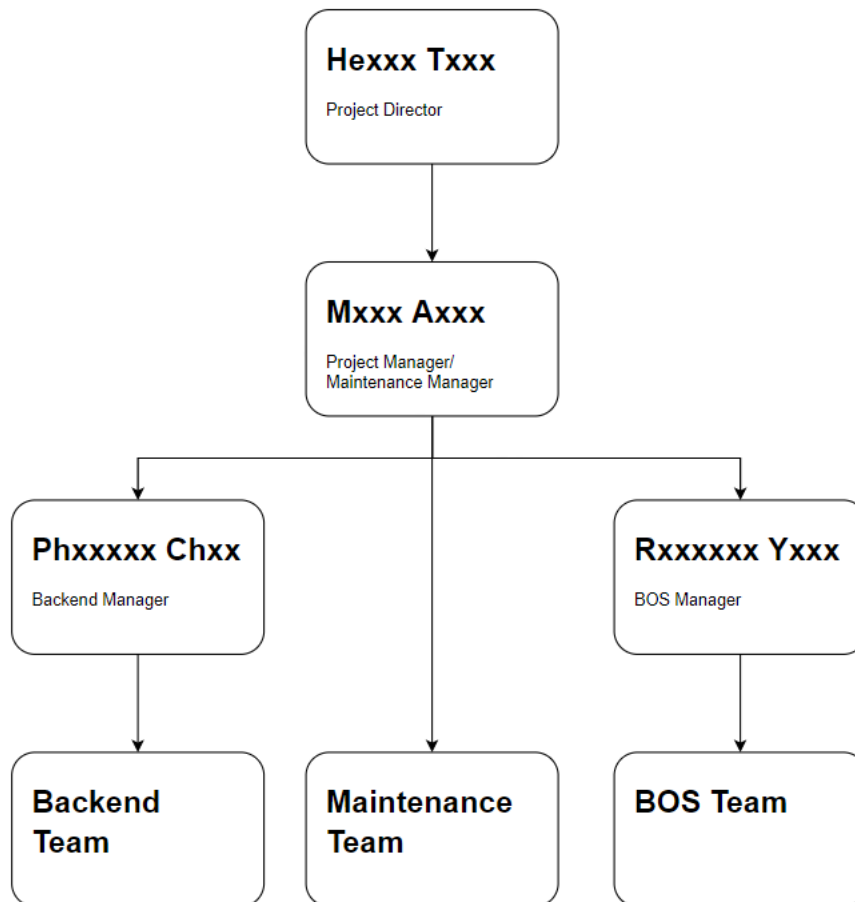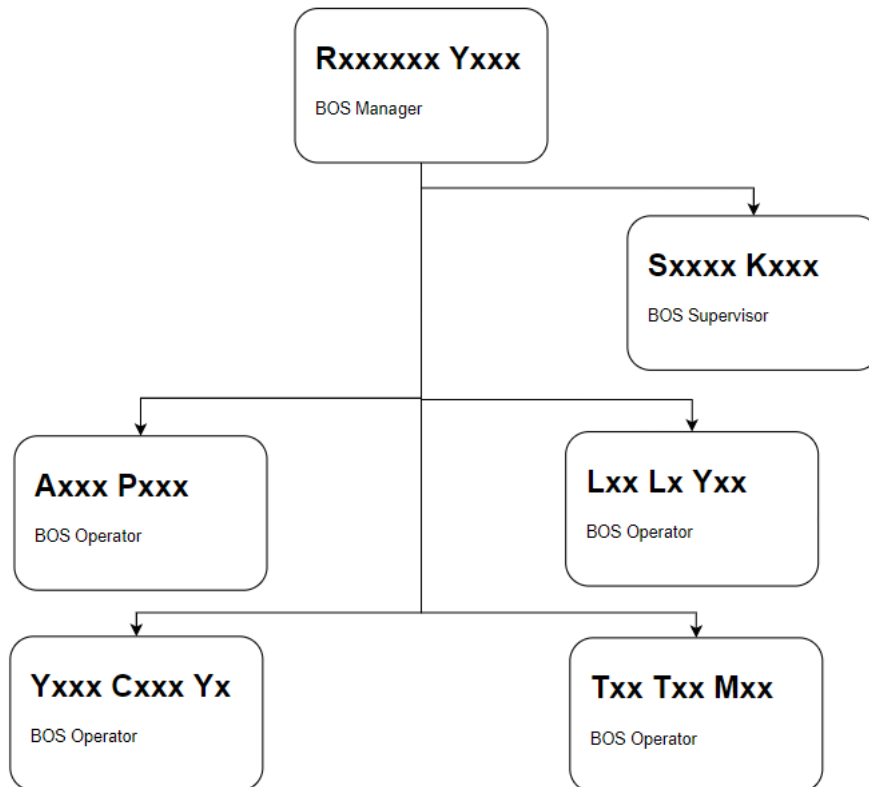
Annex D
System Administrator Add/Remove Request Report

S/N	System Administrator Request	Reviewed	Date of Review	Reason to add or remove	Remarks
NIL					

Annex E
End Users Access Review Report

Name	Account Role	Account Status	Reviewed	Date of Reviewed
Rxxxxxx Yxxx	BOS Manager	Active	Yes	5 Apr 2024
Sxxxxx Kxxx	Supervisor	Active	Yes	5 Apr 2024
Axxx Pxxx	Investigation Officer	Active	Yes	5 Apr 2024
Lxx Lx Yxx	Investigation Officer	Active	Yes	5 Apr 2024
Yxxx Cxxx Yx	Investigation Officer	Active	Yes	5 Apr 2024
Txx Txx Mxx	Investigation Officer	Active	Yes	5 Apr 2024

Annex F
Vulnerability Assessment Report

NOT APPLICABLE FOR THE REPORTING MONTH

Annex G
Penetration Testing Report

NOT APPLICABLE FOR THE REPORTING MONTH

Annex H
Annual Calendar of Scheduled O&M Activities

Month	Activities	Remark
Apr-24	1. Log Review 2. Preventive Maintenance 3. Account Audit Review	
May-24	1. Log Review	
Jun-24	1. Log Review	
Jul-24	1. Log Review 2. Preventive Maintenance 3. Account Audit Review	
Aug-24	1. Log Review	
Sep-24	1. Log Review	
Oct-24	1. Log Review 2. Preventive Maintenance 3. Account Audit Review	
Nov-24	1. Log Review	
Dec-24	1. Back up and Restoration 2. Log Review	
Jan-25	1. Log Review	
Feb-25	1. Log Review	
Mar-25	1. Back up and Restoration 2. Log Review	
Apr-25	1. Log Review	

Annex I
Audit Logs Review Report

S/N	Logs Type	Review Date	Abnormalities	Action Taken	Log Status
1	Application	05-Apr-24	No	Check Logs	No Anomaly found
2	OS	05-Apr-24	No	Check Logs	No Anomaly found
3	Middleware	NA	NA	NA	NA
4	Network	05-Apr-24	No	Check Logs	No Anomaly found
5	Database	05-Apr-24	No	Check Logs	No Anomaly found

Annex J
Log Review For Privileged Users

S/N	Name	Account Role	Reviewed	Date of Review	Reviewer
1	Phxxxxx Chxx	Application administrators	Yes	3 Apr 2024	Hexxx Txxx
2	Phxxxxx Chxx	Database administrators	Yes	3 Apr 2024	Hexxx Txxx
3	Phxxxxx Chxx	OS administrators	Yes	4 Apr 2024	Hexxx Txxx
4	Phxxxxx Chxx	Remote administrators' access	Yes	4 Apr 2024	Hexxx Txxx
5	Phxxxxx Chxx	Firewall administrators	Yes	5 Apr 2024	Hexxx Txxx
6	Phxxxxx Chxx	Network administrators	Yes	5 Apr 2024	Hexxx Txxx

Annex K
Virus Definition Updates Report

NOT APPLICABLE FOR THE REPORTING MONTH

Annex L
Vulnerability Management Report

NO ALERTS RECEIVED FOR THE REPORTING MONTH

Annex M
IT Inventory report

a) Servers

Server Name	Operating System	Server Model	Storage	Firmware Updated Status	EOS/ EOL Status	Roles Installed	AntiVirus
BOSAD01 (.16)	Windows Server 2012 R2 Standard	Dell, R610	-	No Update for this month	2019	Primary AD Server	McAfee VSE 8.8
BOSAD02 (.20)	Windows Server 2012 R2 Standard	Dell, R610	-	No Update for this month	2019	Secondary AD Server	McAfee VSE 8.8
BOSSFTP01 (.11)	Windows Server 2012 R2 Standard	Dell, R310	-	No Update for this month	2019	FTP Server	McAfee VSE
BOSMIS01 (.12)	Windows Server 2012 R2 Standard	Dell, R710	-	No Update for this month	2019	Production CMS	McAfee VSE
BOSMIS02 (.13)	Windows Server 2012 R2 Standard	Dell, R710	-	No Update for this month	2019	UAT Server	McAfee VSE
BOSVR01 (.14)	Windows Server 2012 R2 Standard	Dell, R710	Connect to DAS BOSSTORAGE01	No Update for this month	2019	Sentinel	McAfee VSE
BOSSNMS01 (.17)	Windows Server 2012 R2 Standard	Dell, R710	-	No Update for this month	2019	VCA Server	McAfee VSE 8.8
BOSBACKUP (.21)	Windows Server 2012 R2 Standard	Dell, R710	-	No Update for this month	2019	Image Storage	McAfee VSE 8.8
BOSSTORAGE01	Windows Server 2012 R2 Standard	Dell PowerVault MD1000	RAID6, 22TB	No Update for this month	2019	Images Backup	-
BOSSTORAGE02	Windows Server 2012 R2 Standard	Dell PowerVault MD1000	RAID6, 22TB	No Update for this month	2019	Images Backup	-

Server Name	Operating System	Server Model	Storage	Firmware Updated Status	EOS/ EOL Status	Roles Installed	AntiVirus
BOSNAS1 (.22)	Linux Kernel QTS 5.10	QNAP TS-EC1680U	22TB	No Update for this month	2020	Video & Data Backup	McAfee VSE 8.8
HIKVISION NVR01	Linux Kernel	DS-96128NI-I16	44TB	No Update for this month	2027	24/7 Video Storage	NA
HIKVISION NVR02	Linux Kernel	DS-96128NI-I16	44TB	No Update for this month	2027	24/7 Video Storage	NA
HIKVISION NVR03	Linux Kernel	DS-96128NI-I16	44TB	No Update for this month	2027	24/7 Video Storage	NA

b) Workstation

Workstation Name	Operating System	Workstation Model	Processors	Roles Installed	AntiVirus
BOSSTATION01	Windows 7 Ultimate, SP1	Dell Inspiron 560	Core2Duo E7500@2.94GHz	TECMS, TSS, Sentinel MVE Viewer 5.0.10	McAfee VSE 8.8
BOSSTATION02	Windows 7 Enterprise, SP1	HP Pavilion P6000 P6680d	i5-650@3.20GHz	TECMS, TSS, Sentinel MVE Viewer 5.0.10	McAfee VSE 8.8
BOSSTATION03	Windows 7 Professional, SP1	Dell Precision T1700	i3-4130@3.40GHz	TECMS, TSS, Sentinel MVE Viewer 5.0.10	McAfee VSE 8.8
BOSSTATION04	Windows 7 Professional, SP1	Dell Precision T1700	i3-4130@3.40GHz	TECMS, TSS, Sentinel MVE Viewer 5.0.10	McAfee VSE 8.8
BOSSTATION05	Windows 7 Professional, SP1	HP Compaq Elite 8300	i5-3570@3.40	TECMS, TSS, Sentinel MVE Viewer 5.0.10	McAfee VSE 8.8
BOSSTATION06	Windows 7 Professional, SP1	HP Compaq Elite 8300	i5-3570@3.40	TECMS, TSS, Sentinel MVE Viewer 5.0.10	McAfee VSE 8.8

c) Network Equipment

Models	Name	EOS/EOL	Firmware Updated Status	Service Tag/Serial Number
Fortigate 100D	BOSFG01	July 2023	No Update for this month	FGXXXDXGXXXXXXXX
Dell PowerConnect 6224P	BOSSW01	July 2023	No Update for this month	XKLXGHX
Dell PowerConnect 6224P	BOSSW02	July 2023	No Update for this month	FXJRXMX
Cisco Router 1941	BOSRT01	Sept 2025	No Update for this month	SN: FGLXXXXXXCX ONT: XXXXXXXXXCDEXA
Cisco Router 1941	BOSRT02	Sept 2025	No Update for this month	SN: FGLXXXXXXCY ONT: XXXXXXXXXBDEXA
Cisco Router 2901	BOSRT03	Sept 2025	No Update for this month	SN: FGLXXXXXXKX
Extreme Networks Summit X460-24p	BOSSW03	June 2028	No Update for this month	XXXXNXXXX2
Extreme Networks Summit X460-24p	BOSSW04	June 2028	No Update for this month	XXXXNXXXX9

Annex N
Patch Management Report

NO PATCHING FOR THE REPORTING MONTH

Annex O
Incident Report

NOT APPLICABLE FOR THE REPORTING MONTH

Annex P
Backup and Restoration Report

Name	Type	Monthly Backup Management – March 2024			
		Backup	Result	Frequency	Comments
BOSSNMS01	Database	Yes	Success	Daily	Daily Database backup
BOSAD01	Server	Yes	Success	Daily	Daily Configuration backup
BOSAD02	Server	Yes	Success	Daily	Daily Configuration backup
BOSSFTP01	Server	Yes	Success	Daily	Daily Configuration backup
BOSMIS01	Server	Yes	Success	Daily	Daily Configuration backup
BOSMIS02	Server	Yes	Success	Daily	Daily Configuration backup
BOSVR01	Server	Yes	Success	Daily	Daily Configuration backup
BOSSNMS01	Server	Yes	Success	Daily	Daily Configuration backup
BOSBACKUP	Server	Yes	Success	Daily	Daily Configuration backup
BOSSTORAGE01	Server	Yes	Success	Daily	Daily Configuration backup
BOSSTORAGE02	Server	Yes	Success	Daily	Daily Configuration backup
BOSNAS1	Server	Yes	Success	Daily	Daily Configuration backup
HIKVISION NVR01	Server	Yes	Success	Daily	Daily Configuration backup
HIKVISION NVR02	Server	Yes	Success	Daily	Daily Configuration backup
HIKVISION NVR03	Server	Yes	Success	Daily	Daily Configuration backup
FortiGate 100D	Network/ Firewall	Yes	Success	Daily	Daily Configuration backup

Annex Q
Storage Media Disposal Report

NOT APPLICABLE FOR THE REPORTING MONTH

Annex R
Change Request Report

NOT APPLICABLE FOR THE REPORTING MONTH

Annex S-1.
System Availability

All the servers achieved 100% availability.

Server Name	Roles Installed	System Uptime	Total Available Operational Hours	System Uptime %
BOSAD01	Primary AD Server	589	589	100%
BOSAD02	Secondary AD server	589	589	100%
BOSSFTP01	FTP Server	589	589	100%
BOSMIS01	Production CMS	589	589	100%
BOSMIS02	UAT Server	589	589	100%
BOSVR01	Sentinel	589	589	100%
BOSSNMS01	VCA Server	589	589	100%
BOSBACKUP	Image Storage	589	589	100%
BOSSTORAGE01	Images Backup	589	589	100%
BOSSTORAGE02	Images Backup	589	589	100%
BOSNAS1	Video & Data Backup	589	589	100%
HIKVISION NVR01	24/7 Video Storage	589	589	100%
HIKVISION NVR02	24/7 Video Storage	589	589	100%
HIKVISION NVR03	24/7 Video Storage	589	589	100%

Annex S1-5
System Performance Reports

13.1   System Operational Availability (SOA):

$$\text{SOA} = \frac{\text{Total Serviceable Time}}{\text{Total Available Operational hours}} \times 100\%$$

13.2   Total Available Operational hours for:

Frontend System = No. of CCTV Camera x 19 hours x No. of days

BOS   = No. of BOS x 19 hours x No. of days

13.3   Total Serviceable Time:

Total Available Operational hours – Total Downtime

13.4   For the month of March 2024

System	Total Camera / Equipment	Total Available Operational Hours	Total Downtime (hrs)	Total Video Loss (hrs)	Total System Availability (%)	LTA Requirement (%)
BOS	1	589	0	0	100	99

Annex S-2
Windows System Resource Utilisation

The CPU, memory and disk utilisation were overall healthy.

Server Name	Operating System	Roles Installed	CPU Load %	Memory Load %	Network Load %
BOSAD01	Windows Server 2012 R2 Standard	Primary AD Server	15%	17%	19%
BOSAD02	Windows Server 2012 R2 Standard	Secondary AD server	18%	20%	17%
BOSSFTP01	Windows Server 2012 R2 Standard	FTP Server	19%	33%	62%
BOSMIS01	Windows Server 2012 R2 Standard	Production CMS	32%	32%	42%
BOSMIS02	Windows Server 2012 R2 Standard	UAT Server	17%	32%	41%
BOSVR01	Windows Server 2012 R2 Standard	Sentinel	36%	56%	75%
BOSSNMS01	Windows Server 2012 R2 Standard	VCA Server	21%	44%	58%
BOSBACKUP	Windows Server 2012 R2 Standard	Image Storage	13%	41%	46%
BOSSTORAGE01	Windows Server 2012 R2 Standard	Images Backup	18%	24%	63%
BOSSTORAGE02	Windows Server 2012 R2 Standard	Images Backup	16%	23%	65%

Annex S-3
Database System Resource Utilisation

This was overall healthy with the average CPU utilisation around 46% for the reporting month.

Server Name	Database Instance Name	Database Type	Uptime	CPU Load %	Memory Load %
BOSNMS01	OCS.Vca	SQL Express	100%	46%	36%

Annex S-4
Database System Resource Utilisation

The link bandwidth consumption was overall healthy for the monitored links.

Monitored Link	Uptime	Utilisation
WAN	100%	48%

Annex T
Risk Assessment Report

NOT APPLICABLE FOR THE REPORTING MONTH

Annex U
System Fitness Assessment Report

System is in operation and met the operational availability of 99%