IT SECURITY POLICY

VERSION 1.0

Version	Date	Author	Rationale	Sign
0.1	01.07.16	Anusha Kokil	First Draft	
0.2	18.01.18	Anusha Kokil	First review by Department Head	
0.3	28.03.19	Anusha Kokil	Emtel connectivity added	
0.4	02.05.19	Anusha Kokil	Passwordless authentication by Authenticator Application	
0.5	08.05.19	Anusha Kokil	Security equipment edited	
0.6	12.06.19	Anusha Kokil	Yearly Review by Department Head	
0.7	24.09.19	Anusha Kokil	New network schema, AIP Portal, Security Awareness	
0.8	01.04.20	Anusha Kokil	Mimecast Cloud Security + online Security Awareness Platform	
0.9	20.04.20	Sebastien Pitot	Review of Security Policy document and proposed corrections by COO	
0.91	22.04.20	Anusha Kokil	Corrections done as per COO	
1.0	28.07.20	Sebastien Pitot	Approved by UIL Board	
1.0	28.07.20	Anusha Kokil	Approved by UIL Board	

AXYS

IT SECURITY POLICY

CONTENTS

GOVERNANCE REQUIREMENTS

The AXYS Group should:

1. establish a governance structure that ensures the successful management of protective security risk.
2. appoint a member of senior management to be responsible for the Group policy and oversight of protective security practices.
3. ensure that the individual companies should develop their own set of protective security policies, plans and protocols to meet their specific business needs.
4. conduct an annual security assessment against the mandatory requirements. Policies and plans must be reviewed every two years (or sooner in case of a material change in the existing hardware or software configuration).
5. provide all employees with information and security awareness training to meet the Group Policy Requirements.
6. Implement established procedures for reporting and investigating incidents and taking correction actions.
7. ensure contracted providers comply with the established security protocols.
8. establish a Business Continuity Management (BCM) programme to provide for the continued availability of critical services and assets in the event of a disaster.

GROUP HARDWARE AND SECURITY

Servers & Network

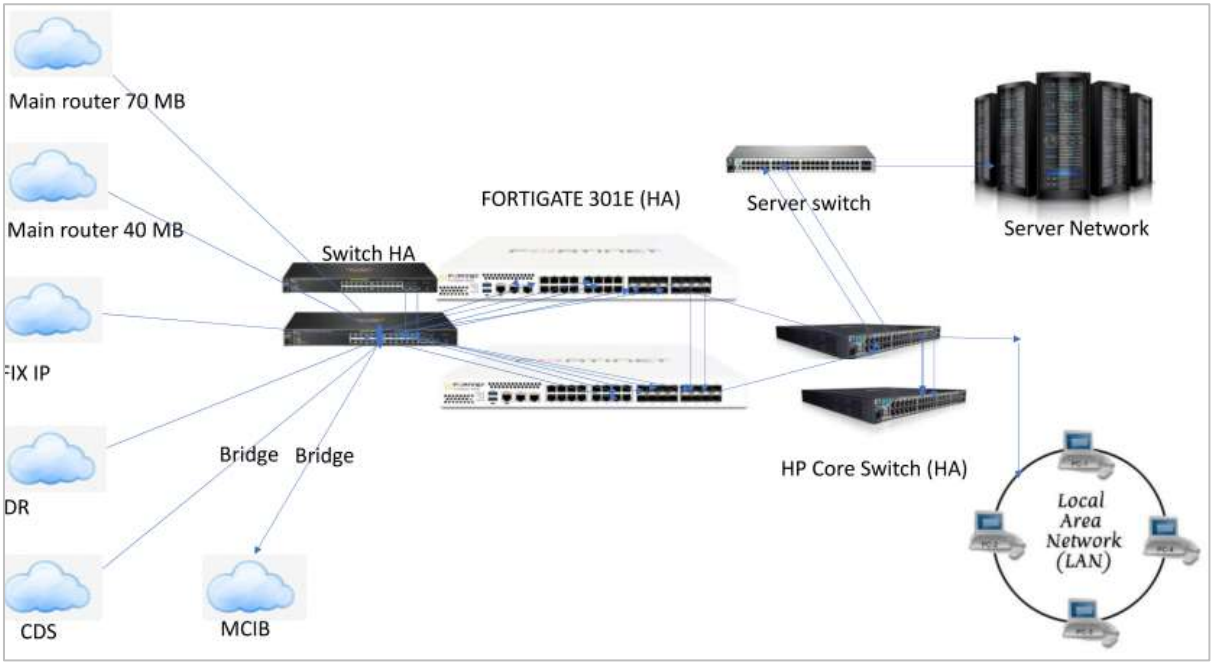
The AXYS Group hardware on the production site comprises of:

1. 2 x Fortigate 301E firewalls in HA and IBM XGS coupled with QRADAR as the latest Intrusion Prevention System as security appliances.
2. HP Switches to regulate the whole core network throughout AXYS Group.
3. 4 x high end HP servers in a cluster with a shared HP storage. VMware vSphere standard 6 with operation management is used as the virtualization platform for High Availability (HA). The whole infrastructure is managed by the VMware vCenter Server Virtual Appliance (VCSA). vSphere Replication (VR) is used to replicate the Group data to the DR site. Several Virtual Machines are deployed with Windows Server 2012 R2 and the main roles are as follows:
    a. Active Domain Controller (***axdc***)
    b. Passive Domain Controller (***axadc***)
    c. File server (***axfs***)
    d. Application server (***axap***)
    e. Terminal servers (***axrds01*** & ***axrds02***)
    f. Security servers

Group applications like Sicorax and Solis reside on ***axap*** and ***axfs*** servers. The users login through the Active Directory on their terminal sessions to access Group applications.

4. Veeam Backup and Replication Enterprise for VMware version 8 is installed on a virtual machine for the daily backup to tape.
5. Aruba Access points with high performance 802.11ac technology deliver secure WPA2-Enterprise WIFI with AES encryption for the authentication of AXYS Group users only.
6. 2 x IBM P8 servers and a shared IBM SAN on which the AXYS Investment Partners Portal resides.
7. A DMZ environment where public facing applications are hosted.

Simplified Network Schema of the AXYS Group Hardware:



Connectivity

The connectivity to AXYS Group is resumed as follows and is under respective SLAs with the telecommunications service providers:

No	Connectivity	SLA	Under
1	Managed WAN VPN to CDS 256 kbps (with managed services)	8H/NBH	ASL
3	IPVPN Pro 70 Mbps (with managed services)	ETRT = 4H 24/7 (GTRS 3)	AXYS Group
4	Emtel Classic Browsing 40 Mbps		AXYS Group
5	IPVPN Biz 6 Mbps (with managed services)	Resilient Backup Activated (BUA)ETRT= 8H 24/7 Total Site Outage (TSO): ETRT= 3H 24/7	AXYS Group
6	EVLL 20 Mbps facing DC Rhill (A-end & B-end)	8H/NBH	AXYS Group
7	EIS Wireless 512 kbps link facing DC Rhill (A-end & B-end)	Backup Line to DR Site	AXYS Group
8	Cloud IP Standby Port (with managed services) – IP VPN Biz 2MB	n/a	AXYS Group
9	Fibre with BOM for MACCS, MCIB, XBRL (with managed services)		SPL
10	ISDN PRA with 300 DIDs	Header: 4054000	AXYS Group

The connectivity lines with managed services are under 24/7 monitoring by the service provider and the failover of the resilient connectivity to the DR site is performed by the latter in case of service disruption.

Network / Security Auditing

Penetration testing is scheduled for every 2 years, with the last one done in June 2020.

User Access & Security

Standards

1. Each user will have a uniquely assigned User ID to enable individual authentication and accountability.
2. For AXYS employees, authorisation from the employee's Head of Department and Human Resources is required for the User ID be issued or revoked. In most cases, this request comes from an automated employee process triggered by the Head of Department or the HR
3. A "generic" User ID that is designated for use by either multiple users or anonymous users, without enabling individual authentication and accountability, is not permitted unless very exceptionally approved by CEO or COO.
4. All such access rights to IT resources shall be recommended by immediate managers.
5. Employees of vendors or service providers, who require access to AXYS Group's systems and other computer resources are subject to authorisation, close supervision, monitoring and access restrictions like that of AXYS staff.
6. Access rights should be reviewed and updated once every six months.
7. Remote access through VPN should be approved by the immediate manager and disabled immediately upon departure of employee.

Access to normal AXYS Group Information

AXYS Group Security Head should ensure that employees, contractors and temporary staff who require normal / specific access to the AXYS Group information and resources:

1. are eligible to have access.
2. are willing to comply with established IT and security policies.
3. have their request for access approved by their immediate managers and sent to the IT department. System users that need to bypass security policies, procedures or mechanisms for any reason MUST seek formal authorisation from their Managers and the COO before sending specific requests for granting, downgrading, or cancellation of a security clearance to the IT department.

Access to AXYS Group Information classified as confidential

AXYS Group Security Head should:

1. execute only formal and approved requests to access confidential information.
2. identify positions that require access to sensitive, confidential, secret and top-secret information.
3. ensure the level of security clearance required to access these are followed.
4. maintain a register of personnel and contractors who hold a security clearance to access this information.

Security Domains

User access to specific security domains is as follows:

Security Domain	Group Network Access	Applications	Data	Users
Untrusted External Network (Internet ,wi-fi)	Through CISCO ASA Firewall to Tipping Point IDS , to SWITCH and into USER LAN in Data Centre	- Office 365 email service	- AXYS Group emails - Group Documents	- Authorised AXYS Group users
	Through CISCO ASA Firewall, to IDS Tipping Point and SWITCH into DMZ	- AXYS Investment Partners Portal	- Customer Data	- Authorised AIP and AXYS Securities users
External Service Provider				
CDS	Dedicated SHDSL to ASA Firewall into Dedicated WorkStation	- CDS Application	- Customer Data	- Designated ASL users
BOM	Dedicated Optical Fibre to ASA firewall to Designated Workstation	- CHEQUE TRUNCATION - MACSS - MCIB - XBRL	- Customer Data	- Designated SFL users
Internal User System				
User LAN	Password based authentication to Group Server LAN and Printer LAN	- Office Application (MS office)	- Respective corporate data	- Authorised Active Directory users with defined access rights
Group Server LAN	Password Authentication	- Office Application (SICORAX, SOLIS, VIEWPOINT, ALTERNATIVESOFT, PAXUS, ..)	- Respective corporate data	- IT Admin Officers - External Service providers
DMZ	CLOSED SYSTEM	- AIP Securities Portal	- Customer data	- None from LAN
CCTV LAN	Independent by Virtual LAN (VLAN)	CCTV System	Image recordings	Designated Users
FAC LAN		MORPHO Fingerprint System	Staff Fingerprints	Designated Users
Telephone LAN	Isolated Network	AVAYA Virtual PBX	User Data	Authorised Group Users

Security Incident Logs

1. Network/Server/Internet/Accounts access are fully monitored 24/7 and regulated by Security devices and outsourced to Megabyte Ltd.
2. Logs of all incidents are stored and available for investigation. Critical alerts are immediately investigated and escalated daily to the AXYS Group IT Department.
3. Any deviation from normal user activity will be flagged and reported to concerned authorities. Any suspicious activity is immediately reported to the AXYS Group IT Department and senior management.
4. Monthly maintenance and updates are performed on security devices to ensure pro-active monitoring on the AXYS Group network against latest threats and security incidents.

Password Management

Passwords are first line of defence, and if not implemented appropriately, are the weakest link in an organisation. The table below resumes the password policy applied for AXYS Group:

Application	Password Required	Minimum Password Length	Password Complexity	Account Lockout if inactive	Lockout Threshold	Password Validity	Expired Password History
Windows Domain Login	Yes	8	Strong: Alphanumeric +special characters	30 mins	5 attempts	90 days	Since first log-in
AIP Portal Servers	Yes	8	Strong: Alphanumeric +special characters Password Generator	30 mins	3 attempts	90 days	3 last passwords
HP Group Servers	Yes	8	Strong: Alphanumeric +special characters Auto Generated	30 mins	3 attempts	90 days	3 last passwords
Oracle	Yes	8	Strong: Alphanumeric +special characters Auto Generated	10 mins	3 attempts	90 days	3 last Passwords

Enforcements:

1. Users are forced to change their initial or temporary passwords upon their first login on the AXYS Domain and Office365.
2. For password reset, a reset request should be sent to the IT Department. To reset the account of another employee, a request with manager approval is enforced.

Accessing Another Staff's User / Email Account

Under exceptional circumstances, it may be required that a staff needs to log into another staff's user / Offcie365 account. Any such requirement should be formally addressed to IT Manager after having been approved from Manager/CEO/COO of respective AXYS Group company.

Security Incidents Handling

In the event of security-related incidents, Megabyte will investigate, and provide a resolution or workaround. Some types of security incidents—such as those caused by Viruses—can often be resolved immediately by Megabytes' Service Desk or maintenance visits. These types of incidents will be handled within the hour.

Electronic Media

Electronic storage media drives (CD, USB) are disabled across all devices to ensure data integrity and security.

Clear Screen Policy

Enforcements:

1. All computers / PC / Thin clients are to be password protected and should not be left logged on when unattended.
2. Computer screens should be angled away from the view of unauthorised persons.
3. The TS session will lock automatically if there is no activity for 30 mins.

Mobile Devices

1. Staffs with mobile office devices (laptops, Mobile phones, Tablets) should not leave any such devices unattended in public places.
2. Mobile Devices will be given access to corporate email and will be monitored via Office 365 Policies which will ensure encrypted and password protected devices for all users.
3. Laptops will have controlled access via AD Group Policies. Users will not be allowed to save any corporate data on any drives on the device. All corporate data will only be accessible via VPN or TS sessions.

Storage

File Server (AXFS)

The AXFS is for file sharing and permissions, storage of terminal user's profile. The AXFS comprises of numerous volumes, including the main Share for the AXYS Group on which all AXYS Group information resides. This is a 1 TB volume, shared by individual AXYS Group companies.

Group Policy Enforcements:

1. Access-based enumeration has been enabled on folder "Share", which displays only the folders a specific user has permissions to access. All other folders are hidden.
2. Documents Redirection whereby each AXYS domain user has their documents folder redirected to the File Server and has offline synchronization to their workstations through Sync Centre. Users are encouraged to keep their documents folder clean.
3. Profiles Redirection is used to redirect each user profile to the file server (AXFS), allowing the user to have the same profile when logging on to any remote desktop terminal session.

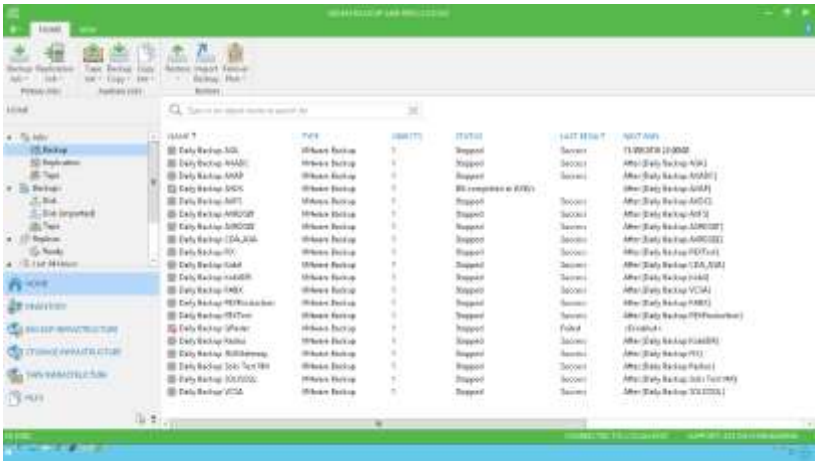
IBM V5000

The AIP Portal has a separate storage, the IBM V5000, of 4 TB. All AIP Portal servers, environments and databases reside on this storage, which is connected to the AIP servers though a dedicated fibre link. On the Live site, this storage is not connected or accessible to any Group server. On the DR site, the IBM V5000 is shared with the Group Infrastructure and all the AXYS Group data and servers reside on this storage.

Backup

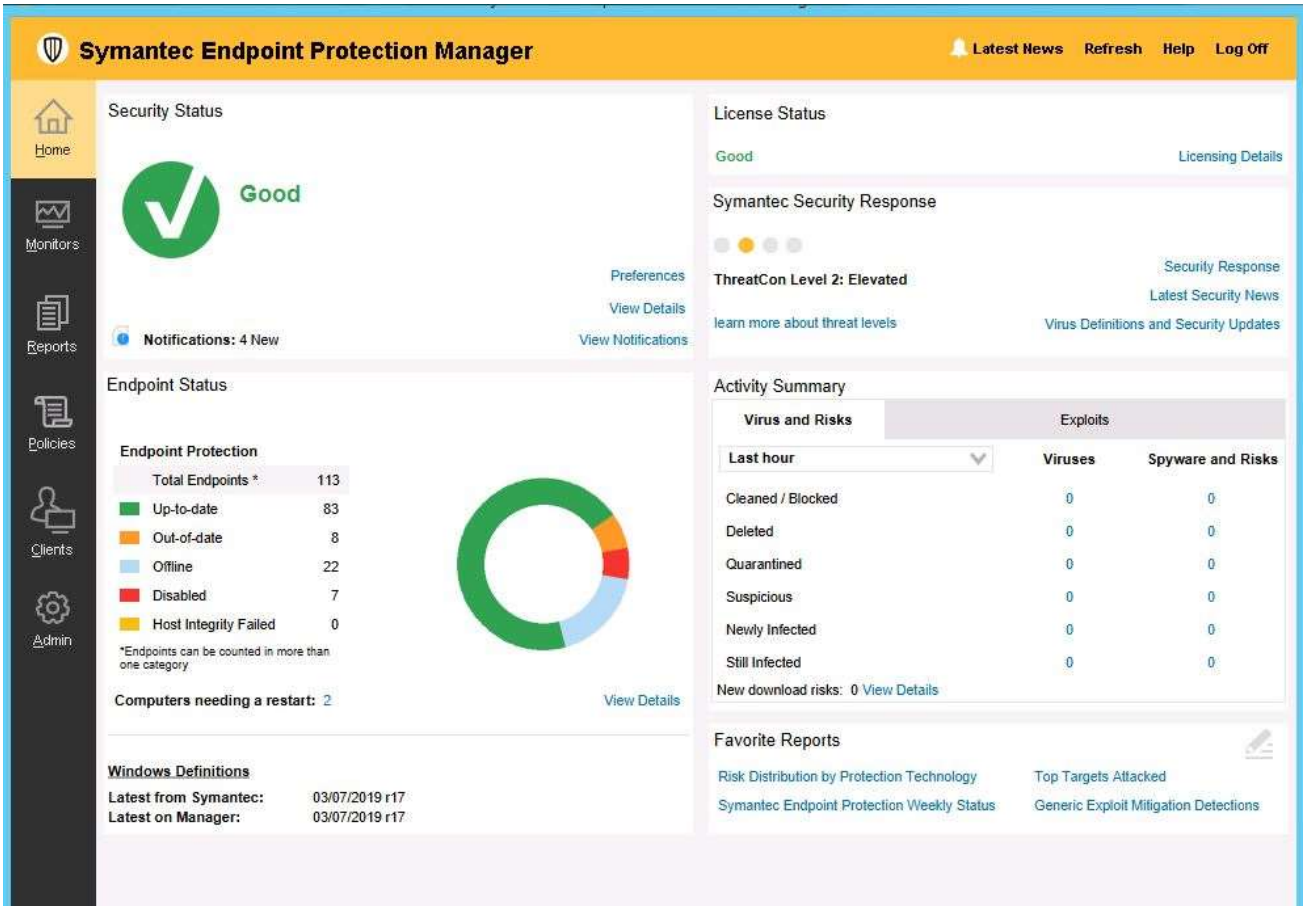
Procedure

Veeam Backup and Replication version 9.5 is used to backup daily all Virtual Machines to a NAS (Synology), which is kept for 2 weeks, and then written to Tape media. The daily backup runs daily at 18 00:



Antivirus Policy

The Symantec Endpoint Protection protects the AXYS infrastructure. The SEP Manager dashboard deployed on the AXDC gives the status of all antivirus protected servers and user PCs / laptops. The Antivirus server checks for live update daily and a weekly scan is scheduled for 11:30 on Friday.



Physical Security

Staff Access

The AXYS Group perimeter is defined as follows:

1. Public and external to AXYS (e.g. Building, lifts, stairs) which is controlled by the Caudan Security Services.
2. Public and internal to AXYS (e.g. Reception area) monitored through CCTV and the receptionists during business hours. This area is separated from the AXYS Offices though fingerprint access control.
3. General employee areas (e.g. Open office areas, mess rooms) controlled by fingerprint access control.
4. Internal sensitive areas (e.g. HR offices, Executive Areas, Board rooms, closed offices).
5. Internal restricted areas (e.g. Server room) monitored through CCTV and by fingerprint access control. An audit trail of access to these areas will be maintained and reviewed by COO on a monthly basis. The store room is always locked and vaults are under dual control and 2-factor authentication.

Visitor Access

Enforcements:

1. Visitors are required to sign a visitor log indicating date, time in, time out, and contact person at AXYS. Visitors are to be escorted at all times through the AXYS offices by their AXYS contact person, wearing a visitor's badge. Visitors should mandatorily go through the reception, before being channelled.
2. All former employees will be treated as visitors and will not be granted any privileged access.
3. Suppliers / vendors access to the server room and data cabinets will be under the constant supervision of the internal IT Staff.

Equipment Security

The following threats have been considered and appropriate controls are implemented to reduce the potential for incident:

Incident	Control	Monitoring Frequency	Incident	Control	Monitoring Frequency
Fire	CO2 Spray	Ongoing / Automatic	Theft	FAC CCTV	Daily
Temperature control	Temperature / Humidity alert system	Real Time	Smoke	Smoke Detectors	Ongoing / Automatic
Dust	Dust free cabinets	Daily	Electrical interference	Surge Protectors	Ongoing / Automatic
Electrical failure	UPS – 5hrs + generator Back up	Ongoing / Automatic	Water	Raised Floor / Temperature / Humidity alert system	Real Time
Inappropriate or unauthorized use	Finger Access Control (FAC)	Daily	Vandalism	FAC; Security Guards	Daily

Security Awareness for employees

The security awareness course for all AXYS Group employees is mandatory and has been conducted once yearly since 2017. However, this had the following limitations:

- Employees might be away from office
- No refresher for joiners throughout the year

As from April 2020, this program now runs on an online platform, available throughout the year with personalised content as per employee behaviour.

MAIL SECURITY

The mail system for AXYS Group resides on the Microsoft public cloud for Office 365. Microsoft Office 365 is a modern collaboration platform that provides a full-featured email system with web access, integrated calendaring, contacts directory, support for mobile device access, and 50 Gb of email storage and 1 Tb of document storage per user account.

The adoption of this platform allows AXYS Group to ensure:

- Business continuity.
- Optimal backup and recovery of the mail system.
- Reduced risk of hacking and mail interception.
- No loss of sensitive data (intentional or accidental).
- Data integrity.
- Efficiency management of the mail system.

Standards

The following controls have been implemented:

- All the individual users' PST files have been centralised, to minimise data loss in case of laptop / user terminal damage.
- The attachment sizes allowed in internal and external communications have been restricted to 800 KB and 10 MB respectively to streamline the volume of mail transiting on the corporate network. Under exceptional circumstances, this limit could be reviewed upward.
- All the mailboxes are journaled to ensure that a copy of each incoming and outgoing mail remains in a hidden mailbox, even if the user deletes the mail from his main mailbox.
- Online archiving has been implemented so that all archives for all users are managed online by Office365 and there is no loss of company data in case of user equipment damage.
- Two factor authentications have been implemented for all users so that a user approves all attempts to connect to his/her Office365 account. Password less authentication is also possible via the Microsoft Authentication application from the user's mobile phone. This adds an additional layer of security to the conventional username and complex password.
- All email attachments were scanned by Microsoft ATP (Advanced Threat Protection) prior to April 2020. Since April 2020, all emails are now scanned by Mimecast Cloud Security for Office365 as the ATP is no longer as efficient as it was supposed to be with new threats.

INCIDENT RESPONSE POLICY

This section details how an incident is communicated to the appropriate personnel, assessment of the incident, minimising damage and response strategy, documentation, and preservation of evidence. The incident response policy will define areas of responsibility and establish procedures for handling various security incidents.

An incident can include but is not limited to:

- Loss of information confidentiality (data theft).
- Compromise of information integrity (damage to data or unauthorised modification).
- Theft of physical IT asset including computers, storage devices, printers, etc.
- Damage to physical IT assets including computers, storage devices, printers, etc.
- Denial of service.
- Misuse of services, information, or assets.
- Infection of systems by unauthorised or hostile software.
- An attempt at unauthorised access.
- Unauthorised changes to organizational hardware, software, or configuration.
- Reports of unusual system behaviour.
- Responses to intrusion detection alarms.

Standards

The incident response life cycle is as follows:

- Discovery (by employees, IDS, administrator, monitoring...).
- Notification of the IT Department.
- Analysis and assessment by Internal IT Department.
- Response strategy (if incident can be dealt with, or escalated to respective vendors)
- Containment to prevent further damage.
- Scan/Check/Restore any affected system/s.

- Documentation to senior management of the incident.
- Evidence of incident preserved and logged in incident report.
- Review response and update policies.

DISASTER RECOVERY SITE

The AXYS Group Live infrastructure run on a VMWARE version 8 virtualised environment. The live infrastructure resides on the AXYS Group servers. Through the firewall, the live site is connected through a 20 Mbps EVLL connection to the DR site at the Mauritius Telecom Rose Hill Datacentre. Through this line, all the Group servers are daily replicated through the VEEAM utility to the DR infrastructure servers. 7 restore points are being kept for critical virtual machines.

The DR has a copy of the AXYS Group whole infrastructure and servers, and the DR site can be activated upon the unavailability of the live site, through the transparent fail-over of fixed IPs. However, there is no provision for war seats for employees to work on the DR site. Once activated, users can connect to the DR site though secure VPN connections.