ISMS EXCERPTS – GENERAL OVERVIEW

aspire SYSTEMS

attention.
always.

WHAT IS INFORMATION ?

Information is an asset which like other important business assets, has value to an organization and consequently needs to be suitably protected

“Information Security is Everyone’s Responsibility”

INFORMATION TYPES

Information exists in many forms:

- ✓ Printed or written on paper
- ✓ Stored electronically
- ✓ Transmitted by post or electronic means
- ✓ Visual e.g. videos, diagrams
- ✓ Published on the Web
- ✓ Verbal/oral e.g. conversations, phone calls
- ✓ Intangible e.g. knowledge, experience, expertise, ideas

“Information Security is Everyone’s Responsibility”

INFORMATION TYPES

Information can be …

- Created
- Owned (it is an asset)
- Stored
- Processed
- Transmitted/communicated
- Deleted / destroy

“Information Security is Everyone’s Responsibility”

INFROMATION CYCLE

Used (for proper or improper purposes)

- ✓ Modified or corrupted
- ✓ Shared or disclosed (whether appropriately or not)
- ✓ Destroyed or lost
- ✓ Stolen
- ✓ Controlled, secured and protected throughout its existence

“Information Security is Everyone’s Responsibility”

WHAT IS INFORMATION SECURITY ?

- ✓ Information security is what keeps valuable information ‘free of danger’ (protected, safe from harm)
- ✓ It is not something you buy, it is something you do
- ✓ It’s a process not a product
- ✓ It is achieved using a combination of suitable strategies
- ✓ and approaches:
- ✓ Determining the risks to information and treating them accordingly (proactive risk management)
- ✓ Protecting CIA (Confidentiality, Integrity and Availability)
- ✓ Avoiding, preventing, detecting and recovering from Incidents
- ✓ Securing people, processes and technology … not just IT!

“Information Security is Everyone’s Responsibility”

INFORMATION TYPES

Information security is defined as the preservation of :

Confidentiality

Making information accessible only to those authorized to use it

Integrity

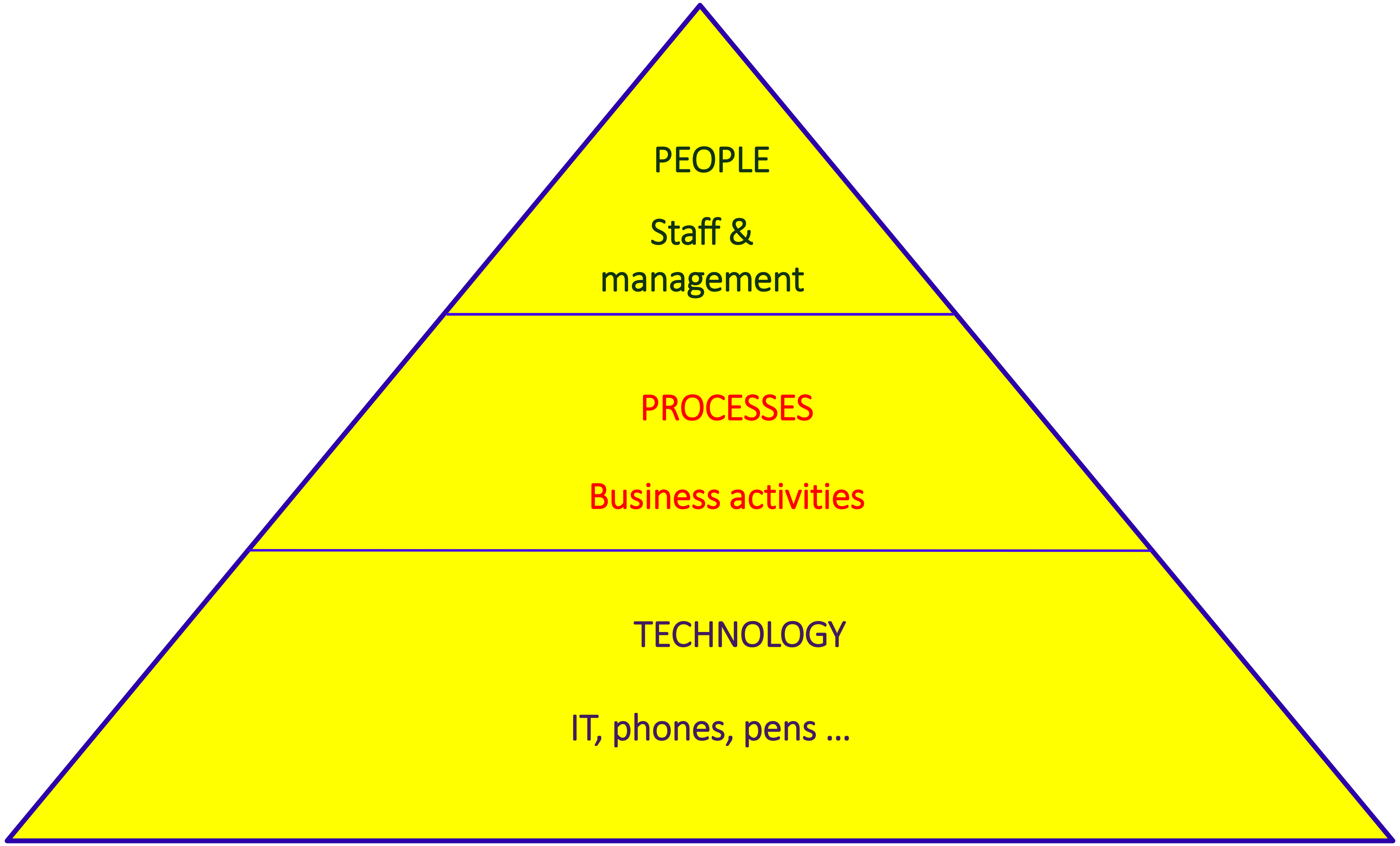
Ensure that information are in format that are true and corrects to its original purpose

Availability

Ensure that information and resource are available to those who need them

“Information Security is Everyone’s Responsibility”

INFORMATION TYPES



PEOPLE

Staff & management

PROCESSES

Business activities

TECHNOLOGY

IT, phones, pens …

“Information Security is Everyone’s Responsibility”

PEOPLE

People who use or have an interest in our information security include:

- ✓ Shareholders / owners
- ✓ Management & staff
- ✓ Customers / clients, suppliers & business partners
- ✓ Service providers, contractors, consultants & advisors
- ✓ Authorities, Governments , regulators & judges

Banks , Insurance companies Our biggest threats arise from people (social engineers, unethical competitors, hackers, fraudsters, careless workers, bugs, flaws, mobile malware, corporate data on personal device …), yet our biggest asset is our people (e.g. security- aware employees who spot trouble early)

“Information Security is Everyone’s Responsibility”

PROCESS

✓ Processes are work practices or workflows, the steps or activities needed to accomplish business objectives

1. Processes are described in procedures
2. Virtually all business processes involve and/or depend on information making information a critical business asset

✓ Information security policies and procedures defines how we secure information appropriately and repeatedly

“Information Security is Everyone’s Responsibility”

TECHNOLOGY

- ✓ Information technologies
- ✓ Cabling, data/voice networks and equipment
- ✓ Telecommunications services (PABX, VoIP, ISDN,
- ✓ Videoconferencing)
- ✓ Phones, cell phones, PDAs
- ✓ Computer servers, desktops and associated data storage devices (disks, tapes)
- ✓ Operating system and application software
- ✓ Paperwork, files
- ✓ Pens, ink
- ✓ Security technologies
- ✓ Locks, barriers, card-access systems, CCTV

“Information Security is Everyone’s Responsibility”

VALUES

- ✓ Protects information against various security threats
- ✓ Ensures business continuity
- ✓ Minimizes financial losses and other impacts
- ✓ Optimizes return on investments
- ✓ Creates opportunities to do business safely
- ✓ Maintains privacy and compliance

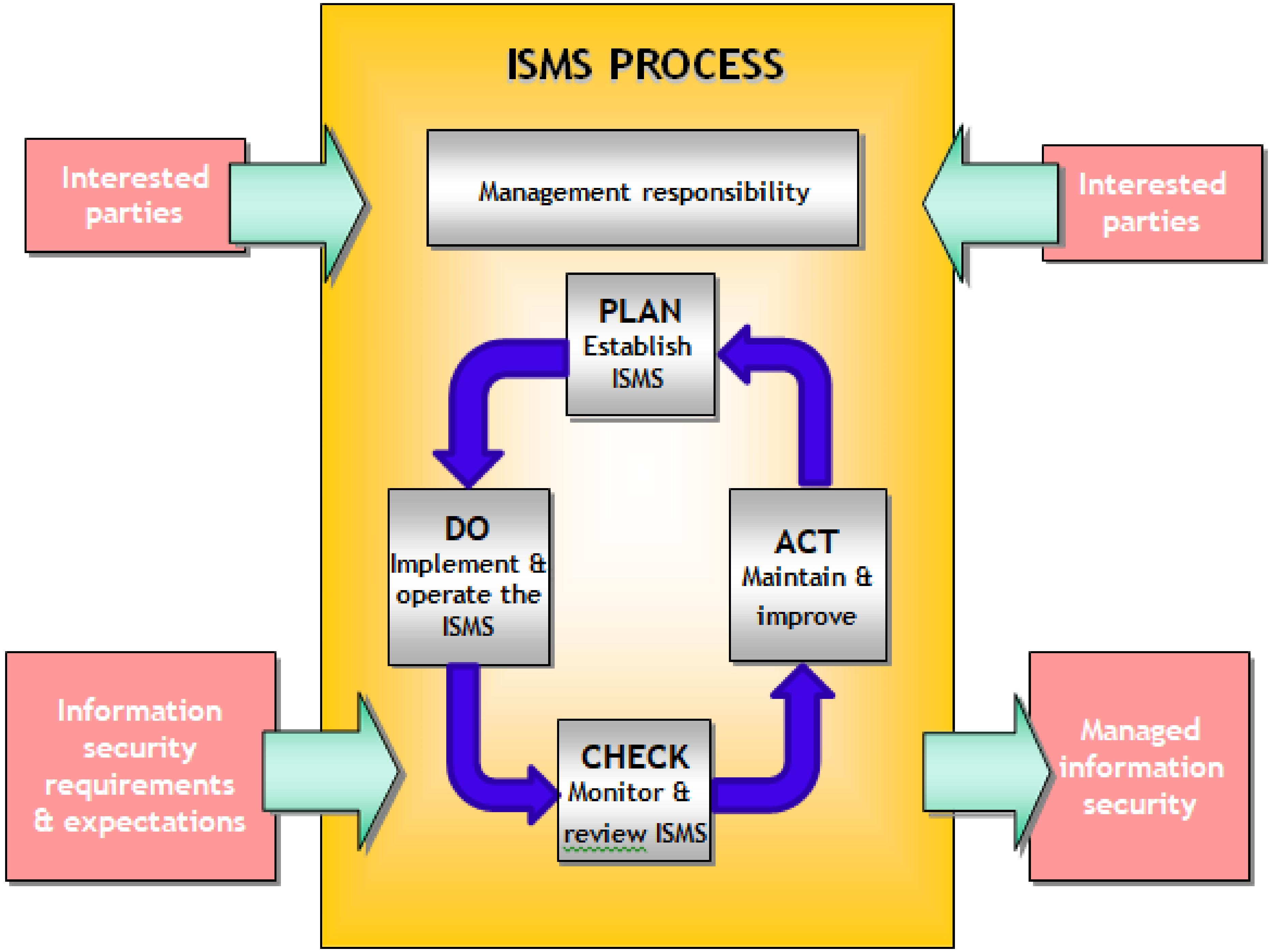
“Information Security is Everyone’s Responsibility”

INTRODUCTION TO 27K

- ✓ Concerns the management of information security, not just IT/technical security
- ✓ Formally specifies a management system
- ✓ Uses Plan, Do, Check, Act (PDCA) to achieve, maintain and improve alignment of security with risks
- ✓ Covers all types of organizations (e.g. commercial companies,
- ✓ government agencies, not-for-profit organizations) and all sizes
- ✓ Thousands of organizations worldwide have been certified compliant
- ✓ It protects the employees identity by defining clear rules and methods for authentication, and for protection of identity data - therefore, the chance that someone's identity is going to be misused is much lower.

“Information Security is Everyone’s Responsibility”

PDCA CYCLE FOR ISMS IMPLEMENTATION


ISMS PROCESS
Interested parties
Management responsibility
Interested parties
PLAN
Establish ISMS
DO
Implement & operate the ISMS
ACT
Maintain & improve
CHECK
Monitor & review ISMS
Information security requirements & expectations
Managed information security

"Information Security is Everyone's Responsibility"

INFORMATION SECURITY METRIC

Information Security Metrics

Aspire Systems has defined the information security metrics for

mainstreams and support services.

Following, Information security metrics for development and testing was introduced

a. % of Ontime Removal of Access
b. % of Ontime Return of Assets
c. Security Defect Leakage

This can be found in the Metrics Analysis Plan

Security requirements for the applications can be found in Non- Functional Requirement document. If required, this can be monitored as new metric for the project.

"Information Security is Everyone's Responsibility"

INFORMATION SECURITY POLICY STATEMENT

Information Security Policy Statement

Aspire Systems is a global technology services firm serving as a trusted technology partner for its customers. Aspire Systems focuses on Service lines that include Product Engineering, Independent Testing, Enterprise Transformation and Infrastructure Application Support.

The Management and all employees of Aspire Systems are committed to an effective Information Security Management System in accordance with its strategic business objectives

“Information Security is Everyone’s Responsibility”

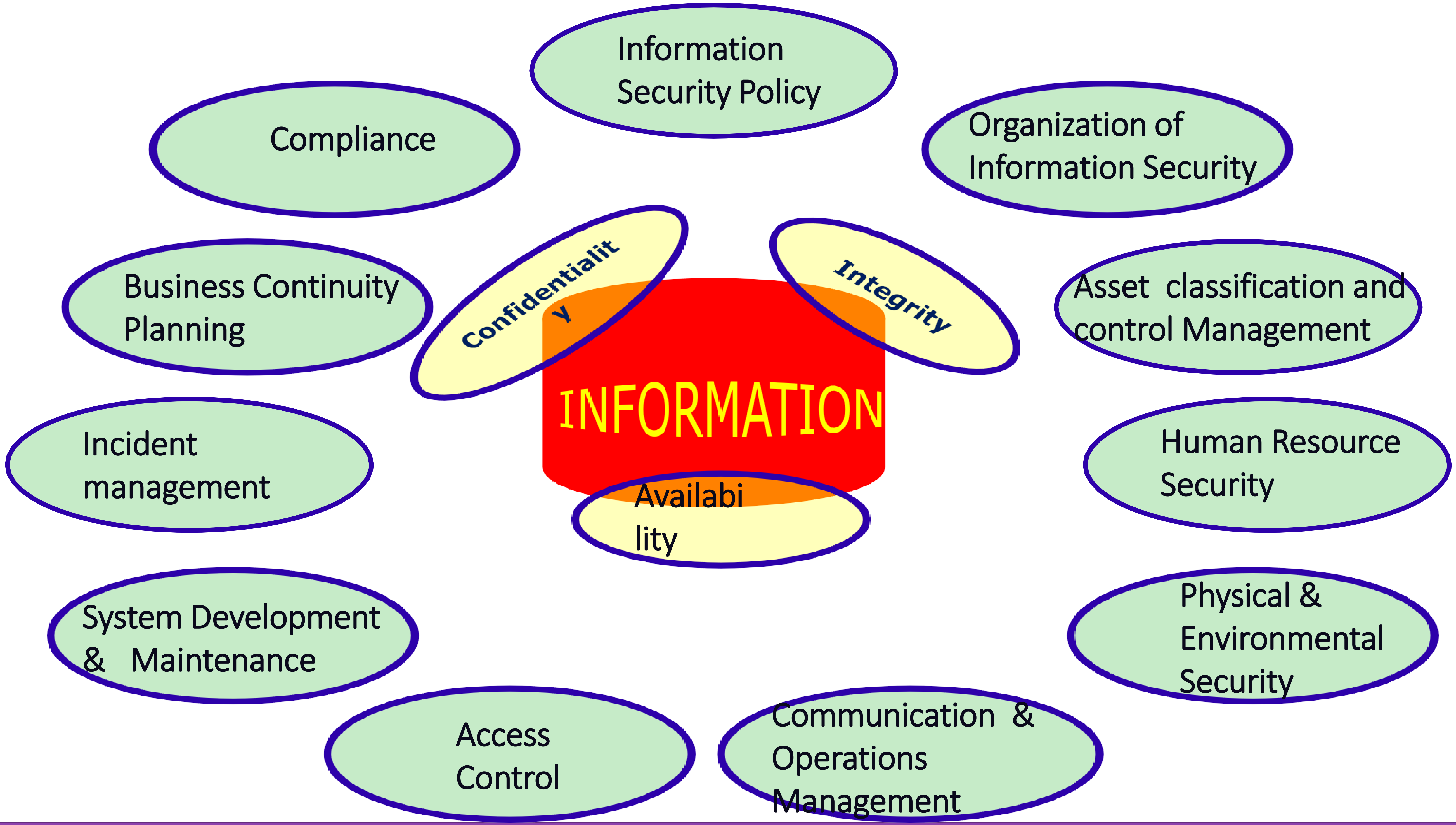
INFORMATION SECURITY POLICY STATEMENT (CONT)

To achieve the above, Aspire shall:

- ✓ Establish and implement policies, processes and the right organization structures (Information Security Management System) to protect the information assets of Aspire and its customers from threats, both external as well as internal.
- ✓ Continually improve the Information Security Management System by adopting a life cycle approach through the establishment and regular monitoring of measurable security objectives.
- ✓ Commit to comply with business, legal, regulatory and contractual security obligations, as may be applicable from time to time.
- ✓ Ensure confidentiality, integrity and availability of the information assets of its customers and other Stakeholders.
- ✓ Develop, implement test and maintain a Business Continuity Plan.
- ✓ Create mechanisms to identify and review the risk and impact of breaches in protected information assets
- ✓ Communicate all pertinent security policies to employees, customers and other interested parties as applicable.
- ✓ This policy applies to all employees of Aspire systems and other users of Aspire’s information processing facilities. The Management and employee shall ensure that this policy is implemented, communicated, monitored and maintained at all levels of the organization and regularly reviewed for compliance and continual improvement.

“Information Security is Everyone’s Responsibility”

CONTROL CLAUSE


Information Security Policy
Organization of Information Security
Asset classification and control Management
Human Resource Security
Physical & Environmental Security
Communication & Operations Management
Access Control
System Development & Maintenance
Incident management
Business Continuity Planning
Compliance
Confidentiality
Integrity
INFORMATION
Availability

“Information Security is Everyone’s Responsibility”

CONTROL CLAUSE

- ✓ **Information security policy** - management direction
- ✓ **Organization of information security** – management framework for implementation
- ✓ **Asset management** – assessment, classification and protection of valuable information assets
- ✓ **HR security** – security for joiners, movers and leavers
- ✓ **Physical & environmental security** - prevents unauthorized access, theft, compromise, damage to information and computing facilities, power cuts
- ✓ **Communications & operations management** - ensures the correct and secure operation of IT

"Information Security is Everyone's Responsibility"

CONTROL CLAUSE

- ✓ Access control – restrict unauthorized access to information assets
- ✓ Information systems acquisition, development & maintenance – build security into systems
- ✓ Information security incident management – deal sensibly with security incidents that arise
- ✓ Business continuity management – maintain essential business processes and restore any that fail
- ✓ Compliance - avoid breaching laws, regulations, policies and other security obligations

“Information Security is Everyone’s Responsibility”

BENEFITS

- ✓ Demonstrable commitment to security by the organization
- ✓ Legal and regulatory compliance
- ✓ Better risk management
- ✓ Commercial credibility, confidence, and assurance
- ✓ Reduced costs
- ✓ Clear employee direction and improved awareness

“Information Security is Everyone’s Responsibility”

CHANGE MANAGEMENT

- ✓ Any changes in the system to be approved by CCB (Change Control Board EX: Project manager , Delivery manager)
- ✓ The Changes are analyzed, tested before implementation
- ✓ The primary goal of the Change management process is to accomplish changes with minimum

  1. Business Impact
  2. Cost
  3. Risk

“Information Security is Everyone’s Responsibility”

CLEAR SCREEN AND CLEAR DESK POLICY / ACCESSING UNAUTHORIZED WEBSITES

- Clear Screen - Computers are to remain locked when you move away from your desk.
- Clear Desk - Don't leave confidential documents on your desk. Confidential documents are to be under lock & key and should not be accessible to unauthorized parties when you move from your desk
- Office desktop/laptop should be handled with care
- While using Desktop/Laptop at home for official purpose, place the systems in a secure environment to avoid mishandling of systems and the information it contains
- While taking photos or videos while working from home, make sure no confidential information is available on your desktop/laptop screen.

- Never visit any unauthorized websites as it leads to malicious attacks.
- Gambling, Porn, Gaming and video streaming sites are few examples among the most vulnerable targets

TECHNOLOGY THREATS

- ✓ **Spyware** is basically any technology that helps gather information about a computer user without their knowledge. **Spyware** monitors user activity on internet and transmit that information in the background to someone else.
- ✓ **Adware** is any software with banner advertisements displayed while it is running.
- ✓ **Malware** is any software that is harmful to a computer user, such as a virus or **spyware.** Malware cannot replicate itself within the system, but can transmit its copies by means of email.
- ✓ **Firewall** is a program or hardware device that filters the information coming through internet connection to a network or computer system.
- ✓ **Switch** is used to connect many devices together on a single computer network.

"Information Security is Everyone's Responsibility"

WINDOWS UPDATE / INSTALLING SOFTWARE APPLICATIONS

- Desktop/Laptops are disconnected from Aspire's Network during working from Home. Hence Protecting individual desktop/laptop becomes crucial; this can be achieved by keeping windows updated with its latest patch versions
- Microsoft releases essential security and other patches for windows machines on second Tuesday of every month
- Manual restart will be required for critical windows security updates/patches to get installed. It is always advised to shut down your system post your work hours.
- Connecting to Aspire's/Client's VPN may be terminated temporarily if latest windows patches are not installed

- Any software application that is not authorized is likely managed without proper patching, updates, configurations, and security protocols. Hence installing unauthorized software increases the risk of outsiders gaining access to official data.
- Installation of approved and authorized software applications can be done only by NSA.
- A cybersecurity finding says – installing torrent application, games, plugins, and any freeware are majorly helping attackers who are constantly looking for vulnerable targets to hack.

UNAUTHORIZED STORAGE OF INFORMATION / PHISHING EMAILS & RANSOMWARE ATTACK

- Never connect an external hard drive or a USB to the PC that is connected to the company’s network. This may transfer the virus/malicious program to penetrate inside our office network.
- Never copy any Aspire/Customer information in the external hard disk. This may lead to breach in information security policies.
- Do not download any official data to the personal system. This may lead to breach of information security policy.
- Never copy or host any source code into any unauthorized public repositories (Github, Bitbucket, etc).

- Do not open links or attachments from senders that you do not recognize
- Do not open attachments in the email which contains .zip compressed/executable file types and any other unknown file type
- Do not provide sensitive personal information (usernames, passwords) over mail
- Inspect URLs carefully to make sure they are legitimate and not imposter sites.
- Check before opening suspicious attachments or clicking links in an email that originated from an external source.
- Phishing emails will request sensitive or confidential information.
- Spam email is an unsolicited sales emails
- Phishing can be done through emails, calls and SMS.

WHO IS RESPONSIBLE

- ✓ Information Security Management Committee
- ✓ Information Security Manager/CISO (Chief Information Security Officer) and Department
- ✓ Incident Response Team
- ✓ Business Continuity Team
- ✓ IT, Legal/Compliance, HR, Risk and other departments
- ✓ Audit Committee

Last but not least, **you**!

  - ✓ Note – The detailed Roles and Responsibilities can be found in \\AspireFS\QA\Process\Documents\ISMS\R and R

- ✓ *Information security awareness training or program is meant for Employees, Contractors, Vendors*

“Information Security is Everyone’s Responsibility”

WFH GUIDELINES

WFH Guidelines

- ✓ Work in private area in your home that will help you focus at work.
- ✓ Please log off from all official systems and applications after work completion.
- ✓ Lock your computer when stepping away from the workspace.
- ✓ If you do not have UPS and working from a direct power source/desktop, please save your work regularly to avoid loss of data.
- ✓ Do not screen capture, copy/paste, print, save on storage(such as local/network hard drive, USD, DVD, etc.) any confidential data.

Secure Access and Connectivity

- ✓ Always use private and not public internet access office/client network.
- ✓ Make sure you have an updated antivirus installed and configured with recent patching.
- ✓ Ensure windows firewall is enabled(seek helpdesk support to configure it).

“Information Security is Everyone’s Responsibility”

WFH GUIDELINES

Secure Access and Connectivity

- ✓ Do not access generic and un authorized sites using Aspire laptop/desktop/dongles.
- ✓ Never share your VPN access with your colleagues and do not install any personal software.
- ✓ Do not access sensitive and unauthorized site with VPN connected and never download data from unreliable sources.
- ✓ Do not connect Aspire/customer VPN from untrusted/malware affected PC.
- ✓ Do not use unofficial USB/thumb drives and do not respond to any unknown/unverified mail.

Availability and Work

- ✓ Always adhere to all the company policies and procedures.
- ✓ Maintain accurate and up to date records of hours worked at home.
- ✓ Be available for calls and have faster response time.
- ✓ Enter timesheet everyday without fail.
- ✓ Take reasonable precautions necessary to secure the equipment.
- ✓ Maintain a clear delineation of when you are working and when you are not working and maintain accurate records.

“Information Security is Everyone’s Responsibility”

ISO 27001 ROAD MAP

- ✓ Creating INFORMATION SECURITY AWARENESS
- ✓ Performing RISK ASSESSMENT
- ✓ Performing a Gap analysis
- ✓ Drafting ISMS policies, procedures
- ✓ Training the organization at different levels for the relevant ISMS areas
- ✓ Creating a Business Continuity and Disaster recovery Plan and
- ✓ testing
- ✓ Performing Internal Audits on the systems readiness
- ✓ Closing the findings of the Internal audits on ISMS
- ✓ Undergoing an external Certification Audit
- ✓ Closing findings of the certification Audit
- ✓ Getting certified to ISO 27001
- ✓ Continual governance of the ISMS system

“Information Security is Everyone’s Responsibility”

THANK YOU :)