**XY EYEWEAR**

**Deliverable 1:**

**INFORMATION SECURITY DOCUMENT**

**INSTITUTION NAME**

**COURSE TITLE**

**Submitted by:**

**STUDENT’S NAME**

**Email:** [**studentmail@gmail.com**](mailto:studentmail@gmail.com)

**Student ID:**

**Supervised by;**

**SUPERVISOR’S NAME**

**Date:**

**21st April 2018**

# 1 INTRODUCTION

XY Eyewear ecommerce store is committed to deliver an accurate, reliable and secure service to her customers all over the globe so as to ensure efficiency and effective value delivery. This can only be achieved through provision of stable and secure availability of its website where customers can access a continuous and uninterrupted resource.

## 1.1 POLICY STATEMENT

XY Eyewear information security policy is intended to provide a high level mandatory rules that best describes the practices required to be adapted by the system users; for more secure and stable ecommerce system.

This document is not meant to restrict users but rather protect the company, users and the partners from damaging or illegal actions by them, either with or without their knowledge.

## 1.2 SCOPE

This policy document implies to all the company employees, contractors, consultant and third party system users. It defines the common security requirements for the XY Eyewear ecommerce system that access, create, maintain, process, update and transmit information over the internet.

## 1.3 OBJECTIVES

The main objective of this security policy is to:

* Protect the XY Eyewear information assets through safeguarding its confidentiality, integrity and availability
* Establish effective governance arrangements including accountability and responsibility for information security within the agency
* Maintain an appropriate level of employee awareness, knowledge and skill to minimize the occurrence and severity of information security incidents
* Ensure the agency is able to continue and/or rapidly recover its business operations in the event of a detrimental information security incident.

# 2. POLICIES

## 2.1 OPERATIONAL/COMMUNICATIONS SECURITY POLICY

This policy area is aimed at ensuring accurate operation of the XY Eyewear Information System and resources. It also caters for change of system and facilities to assure a correct implementation without compromising information security.

### 2.1.1 Information Security Incidence Management

Functional System Administrators and users must follow the right process of Incident management for responding, managing, control and recovering from any security incident. The process must involve:

1. A reporting process that includes Functional System Administrators, System Administrators and Information Security Administrators as appropriate
2. When exercising incident management authority, authorized staff must notify senior management of the incident and mitigation activities at the earliest possible time
3. Staff with incident management responsibilities must be appropriately trained and qualified, and their authorization for access to live systems and data delineated formally
4. Processes are established for handling different types of information security incidents, including immediate action for containment, response escalation and contingency plans
5. Incident response processes must be documented, tested and rehearsed regularly to evaluate their effectiveness.

### 2.1.2 Protection from Malware and Mobile Code

System Administrators, Users and Information Security Administrators must protect information systems from malicious code (e.g. viruses, worms) by undertaking such activities as:

1. Installing, updating and consistently using software (e.g. anti-virus or anti-spyware software) designed to scan for, detect and provide protection from malicious code
2. Prohibiting the use of unauthorized software in the organization and over the website by users
3. Checking files, including electronic mail attachments and file downloads, for malicious code before use
4. Maintaining business continuity plans to recover from malicious code incidents

### 2.1.3 Back-up

The purpose of Back-up is to enable the timely recovery of ICT data and information.

System Users, Functional System Administrators, System Administrators and Information Security Administrators must define document and implement a backup management and recovery processes that reflect the availability requirements of information and information systems. This includes:

1. Types of information to be backed up
2. Schedules for the backup of information and information systems
3. Back-up media management (e.g. retention period, pattern of back-up cycles)
4. Back-up monitoring systems or tools Testing

### 2.1.4 Control of Operational Software

System Users, System Administrators and Information Security Administrators must notify Functional System Administrators and other affected parties of operating system changes to allow:

1. Sufficient time for the review and testing of information systems prior to implementation
2. Review of System Security Plans to ensure information systems will not be compromised by the change
3. Information system testing with the changes to the operating system in a separate (i.e. test) environment
4. Update of business continuity plans if required

### 2.1.5 User Account Management

The purpose is to ensure that all access actions are traceable to an identifiable individual or process.

#### 2.1.5.1 User Account Creation

System Users, Functional System Administrators, System Administrators and Information Systems Security Administrators are responsible for managing access to the assets under their control and must implement registration process which:

1. Requires custodians to approve all access rights.

This process should:

1. Ensure access requests are approved by the supervisor/manager of the user requesting access
2. Ensure the reasons for requesting access are consistent with job responsibilities
3. Maintain records of access right approvals
4. Ensure staff understand the conditions of access and when appropriate, have signed confidentiality agreements and accepted the terms and conditions.
5. Ensure access rights are consistent with the functions
6. Ensure accesses are traceable to an identifiable individual or process
7. Ensure each user is assigned a single unique identifier for accessing information systems
8. Ensure each user is assigned a single unique identifier for accessing information systems.
9. Ensure the responsibilities for authorizing access are segregated from the responsibilities for granting access
10. Restrict access by using predefined role permissions
11. Provide secure and separate transmission of the user identifier and password to the user

#### 2.1.5.2 User Account Deactivation / Deletion

System Users, Functional System Administrators, System Administrators and System Security Administrators must formally assign responsibilities and implement processes to:

1. Remove access privileges for employees and users no longer with the Company within 3 working days upon notification or confirmation by Human Resources and Administration Office or notification by the user
2. Promptly review access rights whenever a user changes duties and responsibilities upon notification or confirmation by Human Resources and Administration Office or notification by the user
3. Promptly review access rights whenever the user’s branch or department is involved in significant reorganization upon notification by Human Resources and Administration Office
4. Review access privileges for employees on extended absence or temporary assignments within 3 working days of the change of status upon notification or confirmation by Human Resources and Administration Office or notification by the user
5. Remove access privileges for employees terminated upon notification or confirmation by Human Resources & Administration Office or notification by the user
6. Quarterly check for and remove inactive or redundant user accounts
7. The user has a responsibility of reporting any changes in duties allocated or change of staff number in case the same has not been effected in the affected systems
8. Human Resources & Administration Office should inform ICT Division of any changes in staff terms, staff numbers, departmental/regional transfers and departures of staff from the organization

#### 2.1.5.3 User Responsibility in Account Management

A user has a responsibility of reporting any changes in duties assigned or change of terms (e.g. staff number, transfer or re-deployment) in case the same has not been effected in the affected systems.

A user has a responsibility to ensure that the single unique identifier (user-id/user-name) for accessing

information systems correspond to current payroll number or Human Resources records in the

organization.

**Exception**

Individual users may have multiple identifiers when:

1. Required to meet unique business requirements provided the rationale is documented and approved by the Information Owner or Information Custodian as appropriate.

## 2.2 ASSET MANAGEMENT POLICY

**Purpose:**

The purpose of this policy is to identify and manage Information assets associated with information systems or services in order to provide control and accountability, support strategic planning, enhance critical incident response, system planning, protection, maintenance and recovery.

**Scope:**

This policy applies to information and information technology assets associated with information

systems or services including those affiliated with third parties including all equipment

that is owned or leased by XY Eyewear.

### 2.2.1 Identification of Assets

System Users, Functional System Administrators and Custodians must identify assets under their control. This includes:

1. Software (Application Software, System Software and Computer Programming tools)
2. Hardware
3. Services including computer and communications service, and general utilities
4. All other information assets including: database and data files, contracts and agreements, system documentation, user manuals, training material, operational or support procedures and archived information

### 2.2.2 Documenting and Maintaining Asset Inventories

System Administrators, Functional System Administrators and Information Security Administrators must document, maintain and verify asset inventories on a regular basis, depending on the criticality and value of the assets, and validate the measures taken to protect the assets as part of an enterprise risk management strategy.

The following information should be recorded to facilitate system planning and asset recovery in the event of interruption, corruption, loss or destruction:

1. Type of asset
2. Ownership

### 2.2.3 Responsibilities of Asset Ownership

System Administrators, Functional System Administrators, Information Security Administrators and System Developers are responsible for controlling the production, development, maintenance, use and security of information and technology assets within their jurisdiction.

System Administrators and Functional System Administrators are responsible for:

1. Ensuring the appropriate classification and safeguarding of information and technology systems or services
2. Defining and regularly reviewing access restrictions, classifications and safeguards in accordance with applicable policies
3. Ensuring that appropriate tools for protecting designated assets are available

System Administrators and Information Security Administrators will be responsible for:

1. Overseeing the functioning of information and technology assets
2. Delivery of services in accordance with defined service requirements
3. Regular reporting on designated information and technology assets

## 2.3 HUMAN RESOURCES SECURITY POLICY

## 2.3.1 Statement:

XY Eyewear knows that in order to prevent and reduce the risk of information theft, online fraud, and malicious of information system. Any individual with the access to the system must be up to the task or role. They need to fully understand their roles in ensuring security of information. They need to have only access to the information they require, and access removed when they don’t need.

### 2.3.2 Purpose:

This policy describes the rules that all the employees must follow in order to maintain the best knowledge and skills of the system. Failure to abide by them may lead to disciplinary actions.

### 2.3.3 Scope:

This policy must be implemented by all System Users, Functional System Administrators, System Administrators and Information Security Administrator.

### 2.3.4 Policy:

* 1. All employees of XY Eyewear, whether holding a temporary, fixed-term or open contract, must comply with the information security policy of the University.
  2. All employees are informed that they are required to abide by the policies relating to data protection and information security when they receive their terms and conditions of employment.
  3. If, after investigation, an employee is found to have violated the organization’s information security policy, they may be disciplined in line with the University’s disciplinary process.
  4. Depending on the information security requirements, XY Eyewear may make additional background checks or conduct additional tests during the recruitment process to assess the suitability of candidates for a role.
  5. All employees must undertake information security training during their induction to raise their awareness of the risks and issues associated with handling XY Eyewear information system, and the appropriate safeguards.
  6. All employees will be informed of the need for reporting information security incidents and of the appropriate method for doing so. Periodic reminders will be issued to all employees.
  7. All employees must maintain their knowledge and skills in relation to information security throughout their employment at the University, undertaking training as required.
  8. At the request of the senior manager, access to information or Information systems may be removed.
  9. Employees who leave the organization will have their access privileges terminated in line with the Managing User Access Policy.
  10. On leaving XY Eyewear, employees must return all information assets and equipment belonging to the University.

## 2.4 PHYSICAL SECURITY POLICY

### 2.4.1 Overview

## 2.5 ACCESS CONTROL POLICY

## 2.6 BUSINESS CONTINUITY POLICY

## 2.7 INCIDENT MANAGEMENT POLICY

## 2.8 IMPLEMENTATION

# 2.9 REFERENCES

*Information Security - Human Resources Policy - Information Services, The University of York*. (2018). *York.ac.uk*. Retrieved 22 April 2018, from <https://www.york.ac.uk/about/departments/support-and-admin/information-services/information-policy/index/information-security-human-resources-policy/>

*IT Security Policies Should Include a Physical Security Policy*. (2018). *InfoSec Resources*. Retrieved 22 April 2018, from <http://resources.infosecinstitute.com/security-policies-include-physical-security-policy/#gref>

*Physical Security*. (2018). *Sans.edu*. Retrieved 22 April 2018, from <https://www.sans.edu/cyber-research/security-laboratory/article/281>