**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**

Table of Contents

[1 INTRODUCTION 4](#_Toc512195212)

[1.1 POLICY STATEMENT 4](#_Toc512195213)

[1.2 SCOPE 4](#_Toc512195214)

[1.3 OBJECTIVES 4](#_Toc512195215)

[2. POLICIES 5](#_Toc512195216)

[2.1 OPERATIONAL/COMMUNICATIONS SECURITY POLICY 5](#_Toc512195217)

[2.1.1 Information Security Incidence Management 5](#_Toc512195218)

[2.1.2 Protection from Malware and Mobile Code 5](#_Toc512195219)

[2.1.3 Back-up 6](#_Toc512195220)

[2.1.4 Control of Operational Software 6](#_Toc512195221)

[2.1.5 User Account Management 6](#_Toc512195222)

[2.2 ASSET MANAGEMENT POLICY 8](#_Toc512195223)

[2.2.1 Identification of Assets 8](#_Toc512195224)

[2.2.2 Documenting and Maintaining Asset Inventories 9](#_Toc512195225)

[2.2.3 Responsibilities of Asset Ownership 9](#_Toc512195226)

[2.3 HUMAN RESOURCES SECURITY POLICY 10](#_Toc512195227)

[2.3.1 Statement: 10](#_Toc512195228)

[2.3.2 Purpose: 10](#_Toc512195229)

[2.3.3 Scope: 10](#_Toc512195230)

[2.3.4 Policy: 10](#_Toc512195231)

[2.4 PHYSICAL SECURITY POLICY 11](#_Toc512195232)

[2.4.1 Overview 11](#_Toc512195233)

[2.4.2 Purpose 11](#_Toc512195234)

[2.4.3 Scope 11](#_Toc512195235)

[2.4.4 Physical Requirements 11](#_Toc512195236)

[2.4.5 Responsibilities 12](#_Toc512195237)

[2.5 ACCESS CONTROL POLICY 13](#_Toc512195238)

[2.5.1 Purpose: 13](#_Toc512195239)

[2.5.2 Policy 13](#_Toc512195240)

[2.6 BUSINESS CONTINUITY POLICY 15](#_Toc512195241)

[2.6.1 Overview 15](#_Toc512195242)

[2.6.2 Scope 15](#_Toc512195243)

[2.6.2 Policy 15](#_Toc512195244)

[2.7 INCIDENT MANAGEMENT POLICY 15](#_Toc512195245)

[2.7.1 Business continuity management process 16](#_Toc512195246)

[2.7.1 Business continuity and impact analysis 16](#_Toc512195247)

[2.7.2 Writing and implementing continuity plans 16](#_Toc512195248)

[2.7.3 Business continuity planning framework 17](#_Toc512195249)

[2.7.4 Testing the plans 17](#_Toc512195250)

[2 REFERENCES 18](#_Toc512195251)

# 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.

## OBJECTIVES

The main objective of this security policy is to:

* To ensure XY Eyewear has adequate controls to restrict access to systems and data.
* To protect the XY Eyewear and its information system/website by ensuring availability, confidentiality, and integrity.
* To establish an effective way of governing the arrangements that includes accountability and responsibility for information system security.
* To maintain a high level of employees’ security awareness, skill and knowledge to prevent or minimize the number of occurrences and effects of security threat/incidents
* To ensure XY Eyewear can resist security incident or rapidly recover it’s from the event of a detrimental 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 report writing methodology that includes Functional System Administrators, System Administrators and Information Security Administrators as required.
2. In the process of incident management and control authority, the authorized employee must notify the senior employee or management of the security incident and planned mitigation actions at the earliest time possible.
3. Employees who have the incident management responsibilities at hand needs to be well trained, qualified, and up to the task. Also their access to XY Eyewear data and live systems be formally authorized.
4. Processes are established for handling different types of information security incidents, including immediate action for containment, response escalation and contingency plans
5. The incident management and response methodology must be well developed, tested, and documented and also rehearsed in order to regularly examine their effectiveness.

### 2.1.2 Protection from Malware and Mobile Code

System Administrators, Users and Information Security Administrators must protect information systems from threats and malicious software’s by practicing the following activities:

1. Install, update and consistently use security software that can scan, detect, prevent malicious codes.
2. Use of unauthorized software or software from unknown sources should be highly prohibited and including the one users can use over the website
3. Scanning downloaded files, including e-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

This policy describes the various methods used in physically protecting the physical devices and systems and the person in charge for implementation of the used method.

This Physical Security Policy will help ensure the physical security of organizational computer systems and information by specifying responsibilities for physical security.

### 2.4.2 Purpose

This Physical Security Policy is intended to ensure that physical computer resources and information resources are properly protected physically.

### 2.4.3 Scope

This Physical Security Policy applies to all organizational computer systems and information including printed copies of information which may be sensitive. This policy is effective as of the issue date and does not expire unless superseded by another policy.

### 2.4.4 Physical Requirements

Appropriate access control, environmental, and protective, measures must be in place to properly protect physical computer systems and information resources from physical harm or unauthorized disclosure. These resources include informational assets that are not computer related. All organizational members are responsible for ensuring that information resources and computer systems have proper and adequate physical security.

Access to server rooms must be logged either electronically or on log sheets. The person getting access must be required to log in and the log in requirement must not be voluntary. Places where authentication devices or data storage facilities exist must require access logs records to be maintained.

Removal or addition of equipment must be logged and the Asset Control Policy must be enforced.

Physical controls must be used to be sure equipment cannot be removed or added without proper logging.

All those who have access to where organizational computer systems are must pass a security background check or be escorted by a staff member who has passed a security background check.

Computer equipment that allows access to systems without logical controls such as account login must be protected in rooms with proper physical access controls. These controls must include mandatory logging of access and proper construction of the room to prevent unauthorized break-in. All terminals with no logical controls must be identified and only terminals registered with host computer systems should be permitted access to the host computer.

### 2.4.5 Responsibilities

**Employee Responsibilities**

1. Be alert and aware of suspicious characters in or near organizational premises. Report or challenge suspicious characters or activities as is appropriate and safe.
2. Keep computer equipment in your possession secure at all times whether on organizational premises or away from the organization.
3. Report loss or theft of any sensitive documents, memory storage devices, or computer equipment to management and document it with appropriate forms.
4. Be sure information assets being disposed of are disposed of properly in accordance with the Equipment and Media Disposal Policy.

**Information Technology Staff Responsibilities**

1. Follow appropriate policies and procedures regarding data storage. Be sure to store backed up data at approved off-site locations according to the File Backup and Restore Policy.
2. System administrators must retain system security logs and review logs on a daily basis according to the Server Monitoring Policy. Logs must be retained according to the Audit Trail Policy.
3. Computer Center managers and administrators must keep records of people with access codes, keys, and combinations to secure areas.
4. Computer Center managers and administrators must be sure physical security requirements for the computer center are being followed and that access to facilities and secure areas is properly logged.
5. Auditors must evaluate the computer center policies to determine their effectiveness in providing the desired outcome of keeping the facility secure and environmentally controlled (at least every 6 months).
6. Auditors must periodically audit the computer center (at least every 6 months) to be sure proper policies and procedures are being followed to secure the facility and to keep environmental controls in operation.

## 2.5 ACCESS CONTROL POLICY

### 2.5.1 Purpose:

The purpose of this policy is to maintain an adequate level of security to protect XY Eyewear data and information systems from unauthorized access. This policy defines the rules necessary to achieve this protection and to ensure a secure and reliable operation of XY Eyewear information systems.

### 2.5.2 Policy

1. Only authorized users are granted access to information systems, and users are limited to specific defined, documented and approved applications and levels of access rights. Computer and communication system access control is to be achieved via user IDs that are unique to each individual user to provide individual accountability.
2. Entity Authentication: Any User (remote or internal), accessing XY Eyewear networks and systems, must be authenticated. The level of authentication must be appropriate to the data classification and transport medium.

Entity authentication includes but is not limited to:

• Automatic logoff

• And Unique user identifier

• At least one of the following:

• Biometric identification

• Password

• Personal identification number

• A telephone callback procedure

• Token

1. Workstation Access Control System: All workstations used for XY Eyewear business activity, no matter where they are located, must use an access control system approved XY Eyewear. In most cases this will involve password-enabled screen-savers with a time-out-after-no-activity feature and a power on password for the CPU and BIOs.
2. Disclosure Notice: A notice warning that those should only access the system with proper authority will be displayed initially before signing on to the system.
3. System Access Controls: Access controls will be applied to all computer-resident information based on its’ Data Classification to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.
4. Access Approval: System access will not be granted to any user without appropriate approval.
5. Limiting User Access XY Eyewear approved access controls, such as user logon scripts, menus, session managers and other access controls will be used to limit user access to only those network applications and functions for which they have been authorized.
6. Need-to-Know: Users will be granted access to information on a “need-to-know” basis. That is, users will only receive access to the minimum applications and privileges required performing their jobs.
7. Compliance Statements: Users who access to this XY Eyewear’s information systems must sign a compliance statement prior to issuance of a user-ID. A signature on this compliance statement indicates the user understands and agrees to abide by these XY Eyewear policies and procedures related to computers and information systems. Annual confirmations will be required of all system users.
8. Audit Trails and Logging: Logging and auditing trails are based on the Data Classification of the systems.
9. Confidential Systems: Access to confidential systems will be logged and audited in a manner that allows the following information to be deduced:

• Access time

• User account

• Method of access

• All privileged commands must be traceable to specific user accounts

## 2.6 BUSINESS CONTINUITY POLICY

### 2.6.1 Overview

Disaster Recovery Planning (DRP) and Business Continuity Planning (BCP) is intended to protect mission critical business processes from the effects of major failures or disasters, and to minimize the risk of interruptions to business activities.

### 2.6.2 Scope

This policy applies to all system users of XY Eyewear systems. Business continuity and disaster recovery management is critical for the control of the risk associated with the loss or damage of systems and system related infrastructure.

### 2.6.2 Policy

Each department in XY Eyewear is responsible for current and comprehensive Business Continuity Planning (BCP). When implemented, the Plan should include those procedures and support agreements, which insure on-time availability and delivery of required products and services. Each Plan must be certified annually with the BCP policy compliance process through the BCP team.

## 2.7 INCIDENT MANAGEMENT POLICY

**Statement:**

As XY Eyewear become more involved in online activity the likelihood of security related incidents increases. This is due to the significant number of outside connections, and serves the needs of thousands of people.

**Objective:**

The objective of security incident handling is to reduce the damage from security incidents and malfunctions by having appropriate procedures in place, to address issues as they arise, and also to plan for incidents before they occur.

### 2.7.1 Business continuity management process

Through formal procedures, develop and maintain a business continuity process. The following control objectives must be covered in the design of these procedures:

1. Identify critical business processes
2. Identify risks in terms of their likelihood and impact
3. Obtain suitable insurance
4. Develop and document an appropriate business continuity strategy
5. Develop and document business continuity plans based on the agreed strategy
6. Test and update plans and processes
7. Nominate and assign responsibility for coordinating the business continuity management process.

### 2.7.1 Business continuity and impact analysis

Through formal procedures, implement a business continuity methodology. The following control objectives must be covered in the design of these procedures:

1. Identification of events that can lead to interruptions
2. Risk assessment to consider all business processes, including information processing facilities
3. Estimation of the impact of interruptions in terms of damage and period of recovery
4. Cooperation of all owners of business resources and processes
5. Endorsement of the plan by management

### 2.7.2 Writing and implementing continuity plans

Through formal procedures, ensure business continuity plans are designed to restore critical business operations in required time periods following a failure. The following control objectives must be covered in the design of these procedures:

1. Identification of all responsibilities and emergency procedures
2. Identification of external business dependencies and the contracts and agreements required by the BCP
3. Documentation of agreed procedures and processes
4. Identification of the appropriate training required by staff to handle emergency procedures and processes
5. Testing and updating of the plans following any changes

### 2.7.3 Business continuity planning framework

Through formal procedures, ensure the use of a single framework for all business continuity plans. The following control objectives must be covered in the design of these procedures:

1. Business continuity plans, emergency procedures, communication plans, fallback plans and resumption plans each have nominated owners, who are responsible for all activities associated with the plans
2. Each business continuity plan specifies its activation conditions and those responsible for the plan plans are amended to reflect new requirements
3. Emergency procedures describe the activities that follow an incident
4. Fallback procedures describe the activities to relocate essential business activities or support services to alternative locations, and the recovery steps for business processes
5. Resumption procedures describe the activities required to resume normal business operations
6. Maintenance schedules specify the testing of the plan
7. Roles and responsibilities lists show who is responsible for each component of the plan and backup personnel
8. Training and awareness programs promote understanding and effectiveness of the business continuity processes

### 2.7.4 Testing the plans

Through formal procedures, ensure that business continuity plans are tested. The following control objectives must be covered in the design of these procedures:

1. Testing schedule indicates testing methods and frequencies
2. Appropriateness of test techniques for the specific recovery plan
3. Inclusion in test techniques of discussions, simulations, full tests, technical recovery tests, recovery tests at an alternate site, and testing of supplier facilities and supplier services.

# 2 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>

[1] Harrison M. A., Ruzzo W. L., and Ullman J. D., “Protection in Operating Systems”, Communications of the ACM, Volume 19, 1976.

Access Control Policy and Implementation Guides | CSRC. (2016). Csrc.nist.gov. Retrieved 22 April 2018, from <https://csrc.nist.gov/Projects/Access-Control-Policy-and-Implementation-Guides>

Access Control Policy: Information Technology Services: Loyola University Chicago. (2018). Luc.edu. Retrieved 22 April 2018, from <https://www.luc.edu/its/itspoliciesguidelines/access_control_policy.shtml>

Access Control. (2018). Policy.monash.edu.au. Retrieved 22 April 2018, from <http://policy.monash.edu.au/policy-bank/management/its/security-framework/chapter7.html>

(2018). Retrieved 22 April 2018, from <https://gipnetworks.com/blog/sans-policy-templates-pandemic-and-business-continuity-policy>

Business Continuity and Disaster Recovery Planning. (2018). Policy.monash.edu.au. Retrieved 22 April 2018, from <http://policy.monash.edu.au/policy-bank/management/its/security-framework/chapter9.html>