**XY EYEWEAR**

**Deliverable 2:**

**HUMAN RESOURCE SECURITY STANDARD**

**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. Policy Statement 3](#_Toc512283758)

[2. Objective 3](#_Toc512283759)

[3. Types of Users 3](#_Toc512283760)

[3.1. Temporary, Part-time and Full-time Staffs 3](#_Toc512283761)

[3.2. Third party users and Contractors 4](#_Toc512283762)

[4. Prior to Employment / Engagement 4](#_Toc512283763)

[4.1. Roles and Responsibilities 4](#_Toc512283764)

[4.2. Screening 4](#_Toc512283765)

[4.3. Terms and Conditions of Employment 5](#_Toc512283766)

[5. During Employment/Engagement 5](#_Toc512283767)

[5.1. Information Security Awareness, Education and Training 5](#_Toc512283768)

[5.1.1. Security Awareness Training 5](#_Toc512283769)

[5.1.2. Technical Training 6](#_Toc512283770)

[5.2. Dismissal and Disciplinary Process 6](#_Toc512283771)

[6. Termination or Change of Employment 7](#_Toc512283772)

[6.1 Responsibilities for Termination or Change of Employment 7](#_Toc512283773)

[6.2. Change of Employment 7](#_Toc512283774)

[6.3. Termination of Employment 7](#_Toc512283775)

[6.4. Return of Assets 7](#_Toc512283776)

[6.5. Removal of Access Rights 7](#_Toc512283777)

[7. Responsibilities 8](#_Toc512283778)

[7.1 Human Resources Office 8](#_Toc512283779)

[7.2 Central IT and Departmental IT service owners 8](#_Toc512283780)

[7.3 Information Security Unit 8](#_Toc512283781)

[7.5 Employees and third party users 8](#_Toc512283782)

# 1. Policy Statement

XY Eyewear needs to perform checks and ensure that all system users are well prepared and suitable for Information System and data access XY Eyewear. All users are required to accept the terms on a confidentiality agreement and sign. All system users need to be trained, given the relevant equipment and reminded of the information security best practices after a period of time and continuously.

On termination of the employment contracts, respective users must be removed or their accounts suspended from the information system.

In change of user role, the information system and data access privileges needs to be reviewed and changed depending on the need to know basis.

# 2. Objective

The main objective of this policy standard to XY Eyewear is to control or manage the human resources aspect of information security for employees in the Company.

# 3. Types of Users

For this standard’s purpose, All the Users or individual who access the XY Eyewear website either via back-end or front-end; be it an employee or a contracted individual in aim to performing whichever job activity or function. The staffs are categorized under the following groups:

## 3.1. Temporary, Part-time and Full-time Staffs

These are the individuals who work in XY Eyewear company a management, administrative, general and users support staffs on full-time, part-time and temporary terms.

The Full-time staffs of XY Eyewear must familiarize themselves with their corresponding staff manual and attend regular staff training to be always updated.

All the part-time staffs must have a terms of benefit that are fully in accordance with provision of the stipulated employment service and related task.

And for all the Temporary staffs, their letter of appointment carries the entire terms of employment and benefits and also they are provided with the explanatory note attached for their best understanding.

## 3.2. Third party users and Contractors

XY Eyewear usually contracts other service provider to recruit and employs other staffs on their behalf instead of employing staffs directly.

Also the visitor and guest on the local premise or XY Eyewear website. In case these parties needs to use XY Eyewear information system then they’ll have to use the system within the allowed time and the course of their work or visit session.

# 4. Prior to Employment / Engagement

## 4.1. Roles and Responsibilities

All users with the specified roles and responsibilities for information security must have documented work descriptions, the terms and conditions of employment or service agreement, which defines these security roles and responsibilities.

## 4.2. Screening

The procedures for personnel recruitment for both staffs should include methodology and procedure for appropriate verification process.

The verification checks should include:

1. Application Form Completed for Interview
2. Independent identity checks
3. Availability of professional referees
4. A check for the completeness and accuracy of the applications (applicants’ resumes, application forms), and confirmation of claimed academic and professional qualifications.
5. Checks of criminal records and credit checks, e.g. bankruptcy

It should be verified that all information related to personal verification checks is handled in

accordance with all relevant regulations and legislations.

The application data should be stored in a secured place that can only be accessed by Human

Resources Office department employees. Appropriate authorization shall be obtained if transfer of

application data is necessary.

Where personnel are supplied from another third party organization, the contract with the third party should set out clearly the responsibility of the third party to carry out checks to a similar level, acceptability of person and sub-contracting.

## 4.3. Terms and Conditions of Employment

The terms and conditions of employment and job description should refer the users to them responsibilities for information security in corresponding job description, handbook and/or guide.

XY Eyewear should make available all security relevant aspects of the job to the employee,

including responsibilities applicable to legal requirements, responsibilities related to classified

information, working outside XY Eyewear or outside normal working hours and those

responsibilities that might extend beyond the employee’s contract.

# 5. During Employment/Engagement

## 5.1. Information Security Awareness, Education and Training

XY Eyewear should have some form of induction training, e.g. training course or seminar, web

based training, etc., which is given to all employees and contractors and third party users. The

induction program is required at general security awareness and technical levels.

### 5.1.1. Security Awareness Training

Every employee, and where relevant, contractor and third party user, should be given the basic level

of security awareness training program. General security awareness sharing sessions for all staff

should be organized on a regular basis.

All trainee of the security awareness training program should sit for a quiz before the completion of

the training. The objective of the quiz is to help both XY Eyewear understanding the overall

security proficiency of the staff, and help staff understanding their own security proficiency. Staff

with result below satisfactory may be requested to attend training and quiz again.

### 5.1.2. Technical Training

Those staff members with special responsibilities for information security should be provided with necessary skills. A training plan should be developed for each individual in accordance with the specific knowledge and skills required for the position held.

The training organizer should maintain records of training.

The staff shall update records of education, training, skills, experience and qualifications to the HRO.

## 5.2. Dismissal and Disciplinary Process

XY Eyewear has standards of behavior reasonably expected to be maintained by a staff member commensurate with his/her position. Any breach of such standards will be considered as misconduct;

disciplinary procedures and actions will be used to deal with such cases.

XY Eyewear has four different levels of disciplinary actions:

1. Formal verbal warning
2. Written warning
3. Final written warning
4. Final disciplinary action

Relevant information on dismissal and disciplinary procedures are documented in the following

documents:

1. Relevant section of respective Service Agreement
2. “Dismissal, Disciplinary Procedures and Grievance Procedures” in Staff Handbook applicable to the specific staff
3. Regulations Governing Staff Discipline

Any disciplinary actions taken against the employee shall be filed in his/her personal record.

The contract with the third party should set out clearly XY Eyewear’s right to require changes of

any personnel used, engaged or deployed by the contractor or service provider.

# 6. Termination or Change of Employment

## 6.1 Responsibilities for Termination or Change of Employment

There should be processes in place verifying that all logical and physical access rights are updated or removed when the job function changes or terminates.

## 6.2. Change of Employment

HRO should acknowledge the Employees’ department as soon as the change of employment is

confirmed. Upon confirmation from HRO, the employees’ department shall inform the affected

managers and supervisors. The original access rights of the employee should be suspended or

removed and new access rights should be granted by the manager or supervisor after change.

## 6.3. Termination of Employment

Employees’ department should submit the termination notice or resignation letter to the Human Resources Office as soon as the termination is confirmed. Alternatively, if resignation is submitted to HRO, HRO shall notify Employees’ department as soon as the termination is confirmed. Employee should document knowledge related to current work, and arrange knowledge transfer of the details of the current work.

## 6.4. Return of Assets

XY Eyewear has procedures in place to verify that all assets in the possession of employees are returned when their employment terminates or changes. Employees shall return all XY Eyewear’s properties such as identity card, cards of benefits, door access card, keys, and any other belongings of the company upon or prior to the effective date of termination.

## 6.5. Removal of Access Rights

If an employment terminates, all access rights associated with the employment should be disabled and considered for removal, except some services provided by XY Eyewear to former staff on a courtesy basis or approved by the responsible service owner or controller. Upon employment termination, the HRO should provide the relevant staff information to the IT department in order to disable or remove all staff rights associated with the employee.

This includes rights to log into the XY Eyewear’s staff network, official e-mail account, software system and any other form of permitted access.

# 7. Responsibilities

## 7.1 Human Resources Office

1. Conduct screening
2. Maintain terms and conditions of employment
3. Maintain change of personnel information process
4. Notify information Security service owners to suspend or remove the logical and physical access rights of employee whose employment is terminated or changed

## 7.2 Central IT and Departmental IT service owners

1. Make sure the employee whose employment is terminated or changed returns all IT related assets directly provided by the Information Security service owners, including the termination of their primary accounts based on the service provisioning policies of XY Eyewear.
2. Suspend, remove or transfer of the logical access rights of employee whose employment is terminated or changed based on the requests from the corresponding department

## 7.3 Information Security Unit

1. Work with line managers, head and HRO to allocate roles and responsibilities for information security to employees

## 7.5 Employees and third party users

1. Comply with relevant Policies, Standards and Terms and Conditions related to employment or service
2. Attend the information security awareness training program and complete the related quiz