**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**

# 1 Policy Statement

XY Eyewear company will ensure that individuals are checked to ensure that they are authorised to access XY Eyewear’s information systems.

XY Eyewear will ensure that users are trained to use information systems securely and also ensure that user access to information systems is removed promptly when the requirement for access ends.

# 2. Purpose

XY Eyewear holds large amounts of personal and restricted information. Information security is very important to help protect the interests and confidentiality of the XY Eyewear and its customers. Information security cannot be achieved by technical means alone. Information security must also be enforced and applied by people, and this policy addresses security issues related to people.

The procedures accompanying this policy are split into 3 key stages of a user’s access to information or information systems used to deliver XY Eyewear business:

1. Prior to granting access to information or information systems - checks must be made to ensure that the individual is suitable for access to XY Eyewear information systems.
2. The period during access to information or information systems - users must be trained and equipped to use systems securely and their access must be regularly reviewed to ensure it remains appropriate.
3. When a user’s requirement for access to information or information systems ends (i.e. when a user terminates their employment with the Council, or changes their role so that access is no longer required) - access needs to be removed in a controlled manner

This policy also addresses third party access to Council information systems (e.g. contractors, service providers, voluntary agencies and partners).

# 3. Scope

This policy applies to any person that requires access to XY Eyewear information systems or information of any type or format.

The policy applies automatically to all XY Eyewear System Users and Administrators.

# 4. Definition

XY Eyewear understands that to reduce the risk of theft, fraud or inappropriate use of its information systems, anyone that is given access to XY Eyewear information systems must:

* Be suitable for their roles.
* Fully understand their responsibilities for ensuring the security of the information.
* Only have access to the information they need.
* Request that this access be removed as soon as it is no longer required.

This policy must therefore be applied prior, during and after any user’s access to information or information systems used to deliver XY Eyewear business.

Access to XY Eyewear information systems will not be permitted until the requirements of this policy have been met.

# 5. Risks

XY Eyewear recognizes that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the risks highlighted on the policy document.

Non-compliance with this policy could have a significant effect on the efficient operation of the XY Eyewear and may result in financial loss and an inability to provide necessary services to our customers.

# 6. Applying the Policy

For information on how to apply this policy, readers are advised to refer to Appendix 1.

# 7. Policy Compliance

If any user is found to have breached this policy, they may be subject to XY Eyewear disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from Security Compliance department.

# 8. Policy Governance

The following table identifies who within XY Eyewear is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

* Responsible – the person(s) responsible for developing and implementing the policy.
* Accountable – the person who has ultimate accountability and authority for the policy.
* Consulted – the person(s) or groups to be consulted prior to final policy implementation or amendment.
* Informed – the person(s) or groups to be informed after policy implementation or amendment.

# 9. Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by XY Eyewear.