|  |  |
| --- | --- |
| **Document Name** | **Information Security Policy** |
| **Version** | **0.3** |
| **Last updated by** | **Anjaly T A** |
| **Approved By** | **Inderjit Singh Bedi** |
| **Released on** | **27-09-2022** |

Contents

[1 Introduction 3](#_Toc61457371)

[2 Objective 3](#_Toc61457372)

[3 Scope 3](#_Toc61457373)

[4 Enforcement 3](#_Toc61457374)

[5 Policy 3](#_Toc61457375)

# 1 Introduction

Information is the critical aspect for any organization’s existence and growth. It is of utmost importance that the policy is defined at organizational level to establish the need to secure information and information processing facilities. Access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements.

# 2 Objective

The purpose of this Policy is to prevent unauthorized access to operating systems. This Policy is designed to protect information from unauthorized change, destruction, or disclosure, whether intentional or accidental.

# 3 Scope

The scope of this Policy includes all XTRACAP employees. Each employee is responsible for carrying out his or her responsibilities under this Policy.

# 4 Enforcement

Violations of this Policy include, but are not limited to: accessing information and information processing facilities which the individual has no legitimate access to; enabling unauthorized individuals to access the information; disclosing information in a way which violates applicable policy, Policy or other relevant regulations or laws; or inappropriately modifying or destroying information. Violations may result in access revocation, corrective action up to and including dismissal, and/or civil or criminal prosecution under applicable law.

# 5 Policy

It is the responsibility of Staff to protect information from unauthorized change, destruction or disclosure.

1. You need to complete Xtracap’s security awareness training and agree to uphold the acceptable use policy.
2. If you identify an unknown, un-escorted or otherwise unauthorized individual in Xtracap you need to immediately notify the CISO.
3. Visitors to must be always escorted by an authorized employee. If you are responsible for escorting visitors, you must restrict them appropriate areas.
4. You are required not to reference the subject or content of sensitive or confidential data publically, or via systems or communication channels not controlled by Xtracap. For example, the use of external e-mail systems not hosted by Xtracap to distribute data is not allowed.
5. Please keep a clean desk. To maintain information security, you need to ensure that all printed in-scope data is not left unattended at your workstation.
6. You need to use a secure password on all Xtracap systems as per the password policy. These credentials must be unique and must not be used on other external systems or services.
7. Terminated employees will be required to return all records, in any format, containing personal information.
8. You must immediately notify the IT Infra team in the event that a device containing in scope data is lost (e.g. mobiles, laptops etc).
9. In the event that you find a system or process which you suspect is not compliant with this policy or the objective of information security you have a duty to inform the IT Infra team so that they can take appropriate action.
10. If you have been assigned the ability to work remotely you must take extra precaution to ensure that data is appropriately handled. Seek guidance from the IT Infra Lead if you are unsure as to your responsibilities.
11. Please ensure that assets holding data in scope are not left unduly exposed, for example visible in the back seat of your car.
12. Data that must be moved within Xtracap is to be transferred only via business provided secure transfer mechanisms (e.g. encrypted USB keys, file shares, email etc). Xtracap will provide you with systems or devices that fit this purpose. You must not use other mechanisms to handle in scope data.
13. Any information being transferred on a portable device (e.g. USB stick, laptop) must be encrypted in line with industry best practices and applicable law and regulations. If there is doubt regarding the requirements, seek guidance from the IT Infra Lead.
14. You must allow all Anti-Virus updates on your laptop and must not uninstall the software from your workstations. Any interference in the function of the anti-virus will result in strict action taken against you.
15. Xtracap will never use any Obsolete Software / Hardware
16. The mobile app updates once deployed are mandatory, thus ensuring that no one uses the obsolete app.