# Information Security Process – Baseline Security Controls

## Policy Statement

This Standard supports the {Company} Information Security & Privacy Policy and outlines the mandatory baseline controls to be implemented across all of {Company}’s systems.

## Applicability

Compliance with the controls outlined in this document is mandatory for all {Company} employees, contractors, vendors, and guests.

## Non-compliance

Any instances of non-compliance with the controls outlined in this document should be reported following the procedures outlined in the Reporting Process.

## Scope

The requirements of this standard to all systems that store, process, or transmit {Company} information; or are used to connect to those systems that are used to store, process, or transmit {Company}’s information.

## Controls

1. All systems shall conform to the requirements outlined in the {Company} Information Classification Standard for the level of authentication required based on the information stored on the system.
2. All systems shall separate user functionality from administrative functions.
3. Systems shall be hardened against or incorporate controls to protect against denial of service conditions, including flooding attacks and resource starvation
4. All traffic traversing the boundary to the Internet must terminate on a proxy device or equivalent. Traffic traversing internal security zones must be restricted via firewalls or ACLs to only allow the minimum required for system operation. Known insecure protocols, such as TCP simple services, should never be allowed to traverse these boundaries.
5. All network traffic should be encrypted by default, either via HTTPS, IPSEC, or SSH.
6. Wherever possible, hosts shall be configured with software firewalls that only allow necessary traffic for designed functionality.
7. Any firewall/ network filter shall have a ‘default-deny’ rule.
8. All management and maintenance of production systems shall be done programmatically via Puppet or other scripted means. Direct host access shall only be used in the event programmatic management fails or if troubleshooting is required.
9. Connection to production systems shall only be via user accounts, with escalation to privileged accounts via su or equivalent. Interactive login via root/sa/administrator/etc. shall be disabled wherever possible.
10. All default/test/shared accounts, passwords, or other credentials shall be removed before systems are placed into production.

## Appendices

### Document Management

|  |  |  |  |
| --- | --- | --- | --- |
| Author | Syltor Consulting | Version | 1.0 |
| Date Modified | 30 May 2019 | Approver |  |
| Last Reviewed |  | Reviewer(s) |  |
| Review Cycle | Annual | Next Review Date |  |