1. **Overview**
Regular application of vendor-issued critical security updates and patches are necessary to protect both Corporate Communications, Inc. (CCI) & Client data and systems from malicious attacks and erroneous function. All electronic devices connected to the network including servers, workstations, firewalls, network switches and routers, tablets, mobile devices, and cellular devices routinely require patching for functional and secure operations.

2. **Purpose**
Software is critical to the delivery of services to CCI customers and CCI users. This policy provides the basis for an ongoing and consistent system and application update policy that stresses regular security updates and patches to operating systems, firmware, productivity applications, and utilities. Regular updates are critical to maintaining a secure operational environment.

3. **Scope**
This policy applies to all CCI systems and hardware.

4. Policy

a. **GENERAL**
All system components and software shall be protected from known vulnerabilities by installing applicable vendor supplied security patches. System components and devices attached to the CCI private network & any and all managed cloud networks shall be regularly maintained by applying critical security patches within thirty (30) days after release by the vendor. Other patches not designated as critical by the vendor shall be applied on a normal maintenance schedule as defined by normal systems maintenance and support operating procedures.

b. SYSTEM, UTILITY AND APPLICATION PATCHING
A regular schedule shall be developed for security patching of all CCI systems and devices. Patching shall include updates to all operating systems as well as office productivity software, data base software, third party applications and mobile devices under the direct management of CCI.

c. PATCHING EXCEPTIONS
Patches on production systems (e.g. servers and enterprise applications) may require complex testing and installation procedures. In certain cases, risk mitigation rather than patching may be preferable. The risk mitigation alternative selected should be determined through an outage risk to exposure comparison. The reason for any departure from the above standard and alternative protection measures taken shall be documented in writing for devices storing non-public data. Deviations from normal patch schedules shall require President’s authorization.

d. SECURITY PATCHING PROCEDURES
Policies and procedures shall be established and implemented for vulnerability and patch management. The process shall ensure that application, system, and network device vulnerabilities are:

i. Evaluated regularly and responded to in a timely fashion

ii. Documented and well understood by support staff

        iii. Automated and regularly monitored wherever possible

        iv. Executed in a manner applicable vendor-supplied tools on a regularly communicated schedule

        v. Applied in a timely and orderly manner based on criticality and applicability of patches and enhancements

5. **Audit Controls and Management**
   On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the [CCI] internal systems change management and update procedures. Examples of adequate controls include:

    a. Documented change management meetings and conversations between key stakeholders

    b. System updates and patch logs for all major system and utility categories

    c. Logs should include system ID, date patched, patch status, exception, and reason for exception

    d. Demonstrated infrastructure supporting enterprise patch management across systems, applications, and devices

6. **Enforcement**
   Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

7. **Distribution**
   This policy is to be distributed to all [CCI] staff responsible for support and management.

Revision History

01/01/2022
  - Originated
01/01/2023
  - Reviewed
01/01/2024
  - Reviewed