GBS GLOBAL APPLIED KNOWLEDGE

GBS Patch Management Policy

1. Overview

Regular application of vendor-issued critical security updates and patches are necessary to protect GBS 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 GBS customers and GBS 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 GBS staff who create, deploy, or support hardware, applications and system software.

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 GBS network 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. Patching updates published in the sector journals and news feeds, such as US CERT and Microsoft's 'Patch Tuesday' (monthly) should be actively monitored by the IT Department and strategic issues reported as a standing item to the GBS Resources Committee.

B. SYSTEM, UTILITY AND APPLICATION PATCHING

A regular schedule shall be developed for security patching of all GBS systems and devices. Patching shall include updates to all operating systems as well as office productivity software, data base software, third party applications (e.g. Flash, Shockwave, etc.), and mobile devices under the direct management of GBS IT Department.

Most vendors have automated patching procedures for their individual applications. There are a number of third-party tools to assist in the patching process and the GBS should make use of appropriate management software to support this process across the many different platforms and devices the GBS IT Department supports. The regular application of critical security patches is reviewed as part of normal change management and audit procedures.

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 Managing Director or CEO 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:

- Evaluated regularly and responded to in a timely fashion
- Documented and well understood by support staff
- Automated and regularly monitored wherever possible
- Executed in a manner applicable vendor-supplied tools on a regularly communicated schedule
- 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 GBS internal systems change management and update procedures. Examples of adequate controls include:

- Documented change management meetings and conversations between key GBS stakeholders
- System updates and patch logs for all major system and utility categories
- Logs should include system ID, date patched, patch status, exception, and reason for exception
- 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 GBS staff responsible for support and management.

10th December 2019

8. Policy Version History

Version	Date	Description	Approved By
1.0	11/11/2018	Initial Policy Drafted	Richard Bingley