Global Banking School
+44 (0) 207 539 3548
info@globalbanking.ac.uk
www.globalbanking.ac.uk
891 Greenford Road, London
UB6 0HE

GBS Patch Management Policy

Document title	GBS Patch Management Policy
Oversight Committee	**Executive Board**
Policy lead (Staff member accountable)	Head of IT
Approved by	Executive Board
Approval date	March 2019
Date effective from	March 2019
Date of next review	March 2025
Version	2.0

Related policies

- GBS Data Protection Policy
- GBS Equality and Diversity Policy
- GBS Freedom of Speech Policy
- GBS Anti-Harassment and Anti-Bullying Policy
- GBS Student Disciplinary Policy and Procedure
- GBS Staff Disciplinary Policy
- GBS Email Usage Policy
- GBS CCTV Policy and Procedure
- GBS Social Media Policy
- GBS Whistleblowing Policy

External Reference

1. Information Commissioner's Office, Accessed online at: https://ico.org.uk/
2. UK Public General Acts, *Data Protection Act 2018*, Accessed online at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
3. UK Public General Acts, *Computer Misuse Act 1990*, Accessed online at: https://www.legislation.gov.uk/ukpga/1990/18/contents
4. UK Public General Acts, *Terrorism Act 2000*, Accessed online at: https://www.legislation.gov.uk/ukpga/2000/11/contents
5. UK Public General Acts, *Counter-Terrorism and Security Act 2015*, Accessed online at: https://www.legislation.gov.uk/ukpga/2015/6/section/26
6. GOV.UK Statutory Guidance, *Prevent duty guidance*, Accessed online at: https://www.gov.uk/government/publications/prevent-duty-guidance

7. UK Public General Acts, *The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000*, Accessed online at: https://www.legislation.gov.uk/uksi/2000/2699/contents/made

Contents

Global Banking School Patch Management Policy

1. Policy Statement

1.1. Global Banking School (GBS) recognises 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

2.1 Software is critical to the delivery of services to GBS staff, students 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

3.1 This policy applies to all GBS staff who create, deploy, or support hardware, applications, and system software.

4. System Component

4.1 All system components and software shall be protected from known vulnerabilities by installing applicable vendor supplied security patches. System components and devices attached to 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 GBS Resources Committee.

4.2 **System, Utility and Application Patching**

4.2.1 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.

4.2.2 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 GBS should make use of appropriate management software to support this process across the many different platforms and devices supported by GBS IT Department. The regular application of critical security patches is reviewed as part of normal change management and audit procedures.

4.3 **Patching Exceptions**

4.3.1 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 authorisation.

4.4 **Security Patching Procedures**

4.4.1 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. Auto Controls and Management

5.1 On-demand documented procedures and evidence of practice should be in place for this operational policy as part of 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. Monitoring and Review

6.1 This policy may be amended by GBS at any time and will be reviewed annually to ensure it is fit for purpose. Any issues related to the monitoring and review of this policy, please contact asgo@globalbanking.ac.uk. Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

7. Data Protection and Confidentiality

7.1 GBS is registered with the Information Commissioner's Office as a Data Controller. Details of the School's registration are published on the Information Commissioners website. GBS as a Data Controller shall implement appropriate technical and organisational measures to ensure that processing of personal information is performed in accordance with the UK General Data Protection Regulations (UK GDPR) and under the Data Protection Act 2018 (DPA).

7.2 The UK GDPR and DPA regulates the use and storage of personal information (i.e., any information which identifies a living individual) on computing systems. It is the user's responsibility to ensure that their information and computer usage complies with this law.

8. Alternative Format

8.1 This policy can be provided in alternative formats (including large print, audio and electronic) upon request. For further information, or to make a request, please contact:

- **Name:** Welfare Management Team
- **Position:** Welfare Officer/Manager
- **Email:** welfare@globalbanking.ac.uk