IT Systems Patching and Vulnerability Management Policy

1 Summary

Security updates must be applied and vulnerabilities addressed within 30 days, or equivalent mitigations deployed, or dispensation formally approved. This includes personally-owned devices. In many cases, enabling automatic updates is the best option. Systems must be regularly checked to confirm that the required updates are being installed.

2 Scope

This policy applies to:

- All systems, including servers, workstations, laptops, tablets, smartphones, network devices, IoT devices, surveillance, door entry and building management systems.
- Both University-owned systems and personal systems that are connected to the University's networks (including wireless) or used for University work.
- All software on these systems, including firmware, BIOS, hypervisor, operating system, drivers, libraries, middleware and applications.

3 Policy

3.1 For many systems, it will be appropriate to enable automatic updates. This is the recommended method for patching personally-owned devices, most workstations, and may also be appropriate for some servers. Whereas in other cases, applying patches manually may be preferable.

3.2 Wherever:

- a vendor / developer releases a patch to fix a security vulnerability, or:
- UofG identifies a vulnerability (e.g. via a network scan)
- a requirement exists to run software unsupported by the vendor / developer

Then the issue must be addressed within 30 days or a dispensation must be obtained in writing (see 3.6).

3.3 Where the risk is assessed as critical (e.g. where attacks on UofG are known to be plausibly imminent or taking place) then the vulnerability must be addressed immediately. The Information Security Team will advise on action to be taken.

3.4 In most cases, installing an update or security patch is the preferred approach to address a vulnerability.

3.5 Where updating or installing patches is not desirable or possible, within the 30-day timeframe, a risk-based approach must be used to determine whether appropriate mitigation measures can be put in place, or alternatively, whether the risk is already mitigated to an acceptable level. This will involve assessing the likelihood of the vulnerability being exploited and the resulting impact on the University should this occur. Mitigations may include physical or logical separation from the network; the Information Security Team will advise what mitigations (if any) can reduce the risk to an acceptable level.

3.6 Vulnerabilities that cannot be mitigated to an acceptable level of risk must be promptly escalated to the Director of IT Services for review. The Director of IT Services under advisement from the Information Security Team may approve a dispensation for the vulnerability, which will be entered into the IT Services risk register and reported to IPSC.

3.7 If none of the above measures are viable then the insecure system will be blocked from accessing the University's data network until an acceptable solution is available.

3.8 Systems must be actively checked to ensure that all required patches are installed; this may involve manual checks, or automated methods (e.g. a monitoring agent installed on individual systems, reporting to a management station). Whichever method is used, all systems must be checked on a regular basis to confirm they are patched as intended, and it is strongly recommended this be done at least every 30 days.

4 Roles and Responsibilities

4.1 The Director of IT Services is accountable for ensuring that all systems are managed in accordance with University IT policies. A quarterly status report will be supplied to the above and the University Information Policy and Strategy committee.

Operational responsibility in section 4.2 rests with

- IT Services. or
- Local IT support staff. or
- the user / owner / research group

In all cases this, and other University IT policies, must be complied with.

4.2 IT staff and any other staff who manage systems and applications are responsible for:

- proactively applying security updates to these systems
- recording changes on the University change control system
- monitoring the security status of their systems, including that the patches which are supposed to be installed have installed correctly
- taking action if they are notified about a specific vulnerability e.g. reported by the Information Security team

4.3 The Information Security Team provide advice on security risks and appropriate measures to deal with them. They also run network vulnerability scans, distribute the results, track actions taken to address vulnerabilities found and ensure escalation takes place where appropriate.

5 Important Notes

5.1 Network scans can identify some vulnerabilities, but cannot identify all vulnerabilities; hence proactive patching is necessary.
5.2 The patches covered by this policy are security updates; installation of feature updates is wholly optional.
5.3 For many systems, it will be appropriate to enable automatic updates. Automatic updates go a significant way to complying with this policy; however, the requirements for monitoring (3.8) still apply.

6 Further information

For further info and advice, please contact your local IT Team, or the Information Security Team.

Title:	Patching and Vulnerability Management Policy				
Version:	1.01	Last Update	2018-09-18	Last Review	-
Author:	Chris Edwards	Status:	Approved by IDGG		