PATCH MANAGEMENT FOR LMBME NETWORKED BIOMEDICAL DEVICE

1. Health Authority Applicability

VCH, FHA, PHC, PHSA.

2. Purpose

Process Objective – Patch Management:

- To regularly monitor and install/remediate vulnerabilities for vendor-approved patches in order to minimize device-related security risk to patients and staff

3. Definitions

Acronym or Word	Definition
Asset	Any equipment managed within the Total Management System (TMS)
Alerts, Hazard Reports, and Recalls	Communications received by LMBME identifying a hazard related to a medical device that may include specific information and actions related to LMBME Risk Management
Alert Log Work Order	Master tracking work order that is created for Alerts that receive intake into LMBME's Hazard Reports and Safety Alerts process
Alert Log	Log of all Alert Log Work Orders. The Alert Log is maintained in TMS and is located in VCH's segment
Alert Group	A procedure-specific team
Alert Chair	A procedure-specific role
Biomed Alerts Meeting	Weekly meeting where the Alert Group reviews new alerts, assigns Alert Coordinators, and reviews alerts requiring follow-up
ECRI	Emergency Care Research Institute
FHA	Fraser Health Authority
IMITS	Information Management and Information Technology Services
LMBME	Lower Mainland Biomedical Engineering
PHC	Providence Healthcare
PHSA	Provincial Health Services Authority
Site Supervisor	A role within LMBME
Supported Groups	VCH, PHC, FHA, PHSA
TMS	Total Management System
VCH	Vancouver Coastal Health

4. Scope

Included:

- Networkable assets for which LMBME has the responsibility to maintain their records are in scope. This is typically in the form of, but not all-inclusive of scheduled maintenance, work orders, alerts, and incidents.

Excluded:

- This process does not replace existing processes for handling provincial hazard and safety alerts. Rather, it refers to this process and should be used in conjunction with it.
- All non-clinical assets supported by IMITS including PCs, Laptops, printers, servers, etc.

5. Guidelines and Protocols

5.1 Procedural Roles

5.1.1 The following roles execute this Standard Operating Procedure:

- Biomed Alerts Group:
  - See full details in the Hazard and Alerts process (SOP # ABCD-14-16-40002)
- Biomed Device Owners:
  - An LMBME team member and/or site supervisor with domain knowledge
  - Technologists to support TMS-related activities
- Biomed Security Group:
  - Discovers alerts, identifies affected inventory, and implements corrective actions
- Biomed Directors:
  - Support process as required, most specifically with general governance
- IMITS:
  - Security team representation to help assess impact of vulnerability and relevance of patch if a device has an IMITS clinical applications
- Patch Deployment Team:
  - Depending on whether the device is biomed or vendor supported, the installation may need to be performed by the vendor and/or a team of biomed resources
- Vendor (Device Manufacturer):
  - Completes any required patch for LMBME as per work order

5.2 Overview of Patch Management Processes

5.2.1 The diagram below covers the six key patch management sub-processes which will be further elaborated in subsequent diagrams:

- Leverage a diverse set of resources to quickly identify patches relevant to your systems
- Perform consistent scanning of IT infrastructure using vulnerability scanners and monitor sources for exposures identified externally
- Embed patching in the SDLC process to insure in-house developed applications are covered
- **Key sources of patches**: Internal threat capabilities, system application scanning, trusted industry sources

- Establish and maintain a prioritization scheme to rank the order in which patches should be applied
- Ideally, deploy every new patch to minimize system exposure according to a risk-based approach
- **Key elements for prioritization scheme**: business criticality, risk rating, vulnerability rating by threat, and age of the patch / vulnerability

- Acquire patch to be applied to devices after ascertaining that the patch has already been validated and approved by both the device vendor and Health Canada
- Create a work order for the vendor if required

- Test patches in an environment that reflects production in order to identify potential disruptions due to patch if not do so already by vendor on device
- Prior to patch deployment, the patch management team should confirm that a rollback plan is defined to address any issues that arise during patch deployment
- **Key patch management release activities**: Test patches prior to release, deploy approved patches to production, and verify successful deployment

- After verifying that a patch will not cause any unintended consequences, the patch management team should deploy the patch to the impacted systems
- For systems for which patches cannot be applied within the appropriate timeframe, implement additional workarounds or alternate mitigation plans

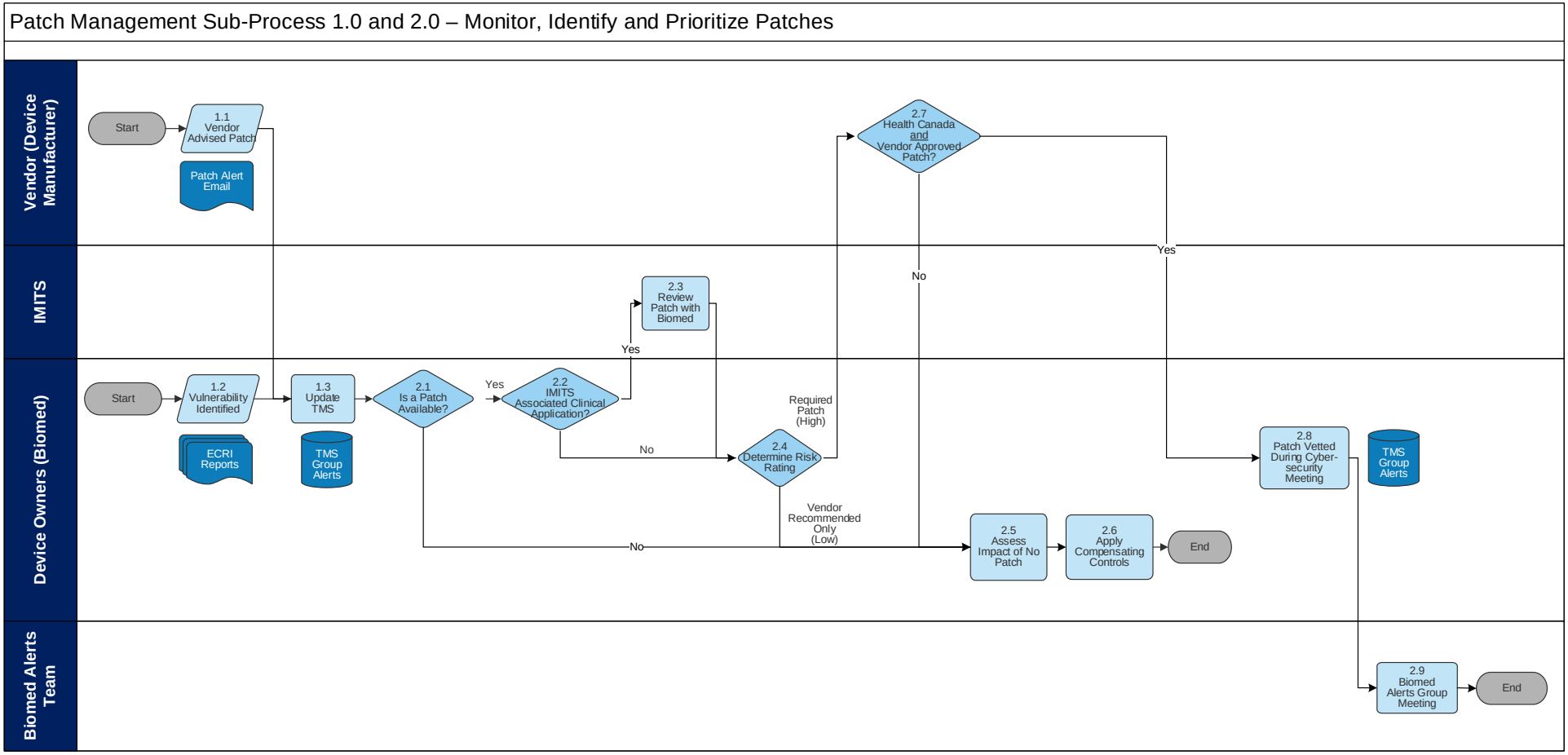
- Multiple methods of verification exist to ensure that patches were applied correctly. Some of the common verification techniques include: rerunning vulnerability scans, reviewing patch logs and performing penetration testing to patched systems
- Dashboards should be created and applicable patches should be monitored until 100% coverage is completed.

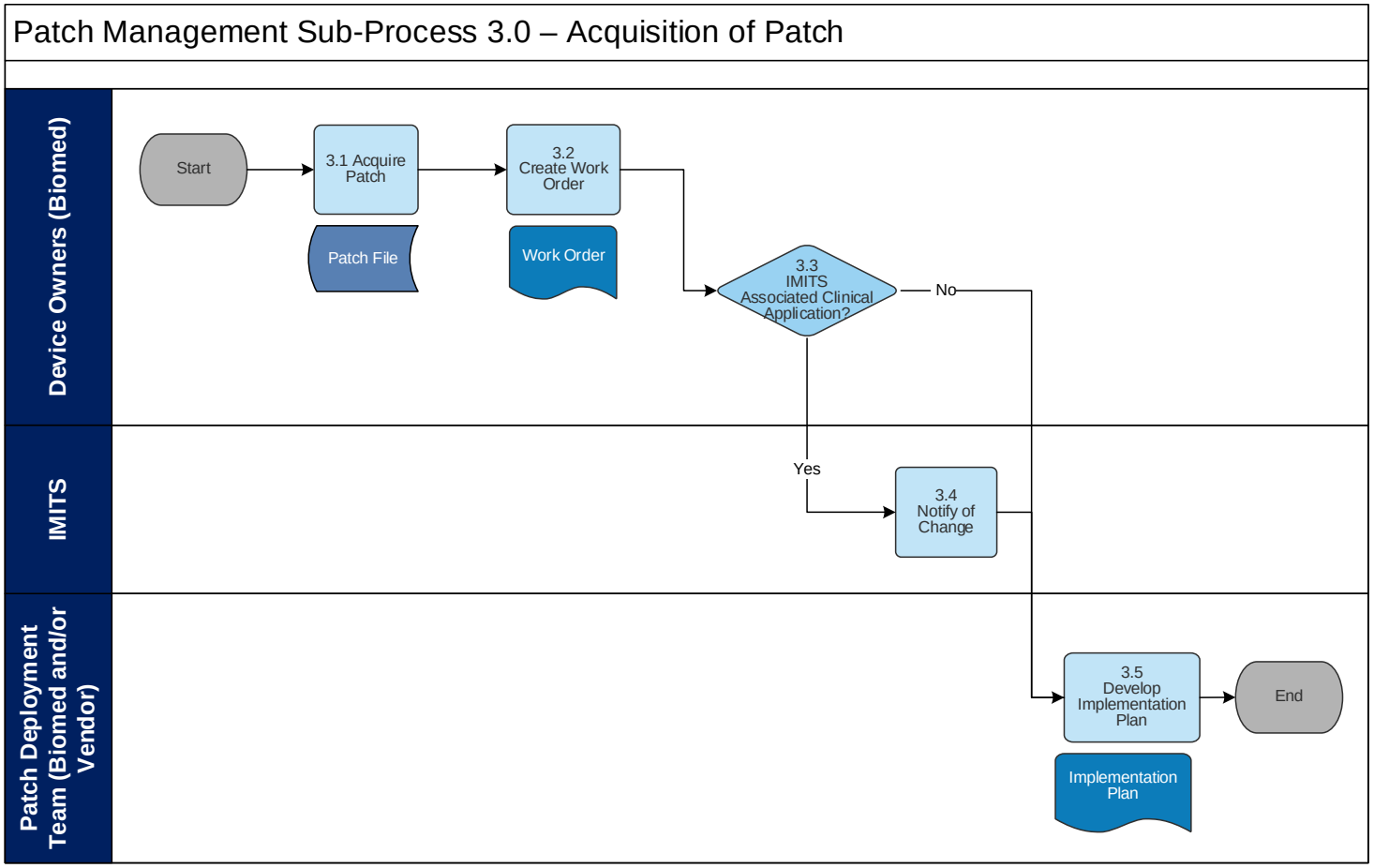
Maintain a Comprehensive System Inventory

- Organizations must know which assets exist in the technology environment in order to protect against vulnerabilities
- System inventories should include risk rating to prioritize which systems, if left unpatched, could result in the highest business impact in the event of a breach

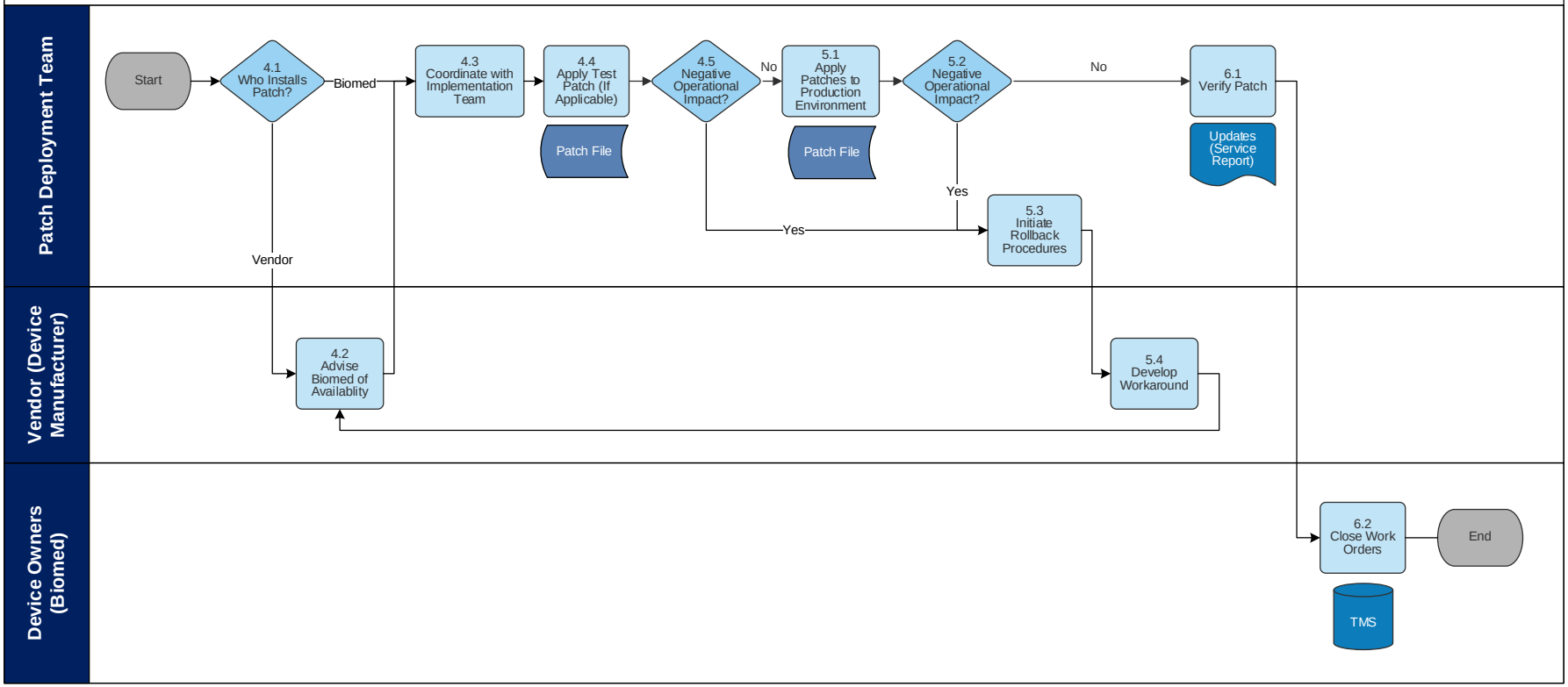
5.3 Patch Management Process Diagrams

5.3.1 Diagram of patch management processes:





Patch Management Sub-Process 4.0 to 6.0 – Test, Deploy, and Verify Patch



5.4 Process Steps

The below table documents the major steps and objective of each process component:

Sub-process	Process Item	Description	Objective	Actors Involved
1.0 Monitor and Identify Patches	1.1	Vulnerability is identified by ECRI	Vulnerability is identified by ECRI via email (dbm.team@vch.ca) to owners. The security alert triggers the need to investigate whether the security alert can and should be addressed.	• Biomed Security Group
	1.2	Vendor Patch Advised	Vendor advises via email (dbm.team@vch.ca) that a patch is required. This alert may or may not be related to the ECRI alerts.	• Vendor • Biomed Security Group
	1.3	Update TMS	TMS is updated manually to reflect the latest list of vulnerabilities provided by ECRI. Alerts of highest importance are named starting with "H" (for Hazard) and are critical but may not necessarily have an available security patch.	• Biomed Security Group
2.0 Prioritize Vulnerabilities / Patches	2.1	Is a Patch available?	It is reviewed whether or not a patch exists to address the vulnerability alert identified by ECRI. If it is not available, the impact of having no patch will be assessed. If it is available, it will be reviewed further.	• Biomed Security Group
	2.2	IMITS Associated Clinical Application	If a patch is available, the device will be reviewed to understand whether or not there is an associated IMITS clinical application. While not applicable in most cases, IMITS must be notified in these cases.	• Biomed Security Group • IMITS
	2.3	Review Patch with Biomed	If the device has an IMITS clinical application, the relevance of the patch will jointly be assessed based on criteria set by PHSA. In all cases, however, if a patch is required by Health Canada it will be considered a priority. The review of patch relevancy is done chiefly by Biomed but with input from IMITS.	• Biomed Security Group • IMITS
	2.4	Determine Risk Rating	The ECRI reports have a risk rating associated to the vulnerabilities which are reviewed by the Biomed Security team, in conjunction with any other correspondence from vendors, Health Canada and other sources to determine the criticality of the risk. If the risk is "required" by Health Canada, it will always be prioritized to patch whereas if it is only "vendor recommended" it may not be prioritized. It is therefore important at this stage to also assess the relevance of the patch as well.	• Biomed Security Group
	2.5	Assess Impact of No Patch with Biomed	If there is no patch available, the impact is assessed for the security alert. This assessment will be done jointly between IMITS and Biomed and may involve Biomed leadership and/or other oversight depending on the impact noted from this step. This step must be done before a risk is accepted.	• Biomed Security Group • Biomed Directors • IMITS
	2.6	Apply Compensating Control	A compensating control is applied if a patch is not applied when applicable. If a control is not documented, the risk is accepted until a control or patch is available. IMITS should be alerted of this issue if not already aware and vulnerability management process followed.	• Biomed Security Group
	2.7	Health Canada and Vendor Approved Patch?	Only patches that have been approved by Health Canada can be applied. This approval may take up to a year depending on the patch. This is the vendor's responsibility. In addition, only vendor approved patches will be applied. This step in most cases also means that the security patch has already been tested by the vendor on their devices before it is used at PHSA.	• Biomed Security Group • Vendor

	2.8	Patch Vetted during Cybersecurity Meeting	**Every Friday,** the Biomed Security team meets internally to vet the patches for vulnerabilities that are of a critical or high nature. Critical Alerts are reviewed here first before the Tuesday province-wide Alerts meeting.	• Biomed Security Group
	2.9	Provincial-Wide Biomed Meeting	**Every Tuesday,** The Provincial Leads that comprise the Biomed Alert Group will review alerts collectively. This team will review all critical Alerts. In all cases, only patches approved by Health Canada and the vendor will be made. Any patch that was deemed 'required' by Health Canada will be prioritized by this team. By the completion of a subsequent meeting for a given approved patch, a work order will be generated in the next step. In some cases, clinicians will be made aware of the patch.	• Biomed Alerts Group • Biomed device owners • Clinicians
3.0 Acquisition of Patches	3.1	Acquire Patch	The patch will be acquired and/or additional decisions will be made as to who will install the patch	• Biomed device owners
	3.2	Create Work Order	A work order will be created to complete the patch. The contract if with a vendor could be in the form of time and materials if outside warranty period. In all cases, whether or not the device is vendor or biomed supported, a work order is needed.	• Biomed device owners
	3.3	IMITS Associated Clinical Application	If there is an associated IMITS clinical application, they will be notified of this change	• Biomed device owners
	3.4	Notify of Change	Biomed should notify the IMITS security team when the patch is to be completed if otherwise not done in the prior step with details of when it will take place. The impact should have already been discussed during step 2.2. If this had not been done due to availability of information, it will be done again in this step.	• Biomed device owners
	3.5	Develop Implementation Plan	An implementation plan is developed based on device type. If this is for a vendor-supported device, this is started before vendor availability is provided as in some cases this might not be readily available. This step is may capture additional project artifacts needed to patch.	• Biomed device owners
4.0 Test Patches Systematically	4.1	Who Installs Patch?	If the vendor is to apply the patch, a work order will be created for the vendor to complete this work either based on the existing contract or time and materials if the device is not in its warranty period. If Biomed supports the device, no work order is needed.	• Biomed Alerts Group
	4.2	Advise Biomed of Availability	The patch is dependent on the vendor's confirmed availability if this is a vendor-managed device which will dictate the date and duration of the patching window for deployment. If a patch done by Biomed for a Biomed supported device requires a workaround, they will require vendor support and their availability to help with the patch.	• Biomed device owners
	4.3	Coordinate with Implementation Team	Ensure alignment with clinicians, IMITS, and other teams in preparation of day-of implementation on-site as necessary.	• Biomed device owners
	4.4	Apply Test Patch	Change is applied to the environment to test if there are any negative operational impacts, or if necessary, initiate a controlled deployment. Note: In almost all cases, testing is not done at this stage because it has already been completed, the impacts are known to the vendor, and patch is confirmed to be safe by Health Canada.	• Vendor • Biomed Technologists
	4.5	Negative Operational Impact?	If there are negative operation impacts, rollback procedures are completed.	• Vendor • Biomed Technologists

5.0 Deploy Patches to Address Vulnerabilities	5.1	Apply Patches to Prod Environment	Patch is deployed by vendor.	• Vendor • Biomed Technologists
	5.2	Negative Operational Impact?	If there are negative impacts to operations, rollback procedures are completed. If not, it will be verified whether patch is complete.	• Vendor
	5.3	Initiative Rollback	Rollback procedures are completed if there are negative impacts of the patch to operations.	• Vendor
	5.4	Develop Workaround	The vendor will need to support the development of a workaround that is safe for the device before it is applied.	• Vendor
6.0 Verify Successful Deployment of Patches	6.1	Verify Patching	The vendor will verify the patch. After completing this, the vendor will send to the device owners a service report once complete that documents findings.	• Vendor
	6.2	Close Work Order	Work orders are closed and records are updated in TMS.	• Biomed Device Owners
	N/A	Audit of findings	For details on how audits of the patch management process are performed to validate the process for verifying success deployments, see Hazard Reports and Safety Alerts (SOP # ABCD-14-16-40002)	• N/A

6. Supporting Files

- Management of Standard Software Patches for VPP (IMITS 340 and IMITS Patch Standard v0-5)
- Hazard Reports and Safety Alerts (SOP # ABCD-14-16-40002)
- Risk Categorization Table - Provincial Preventive Maintenance Program (BCBME SOP005)

Effective Date:	1-JUN-2021			
First Released:				
Last Revised:	9-MAR-2021			
Last Reviewed:				
Approved By:	LMBME Executive Director			
Owners:	Cybersecurity Team			
Revision History: *(optional)*	**Version**	**Date**	**Description/ Key Changes**	**Revised By**
	0.1	29-Jan-2021	Initial Draft	IMITS Security and Biomed Engineers
	0.2	12-Feb-2021	Updated Draft	IMITS Security
	0.3	12-Feb-2021	Updated Draft	Biomed Supervisor
	0.4	19-Feb-2021	Updated Draft	Biomed Engineers
	0.5	08-Mar-2021	Updated Draft	Biomed FHA Director
	1.0	09-Mar-2021	Updated Draft	Biomed VCH Director