

Unclassified Computer Security Variance Request and Approval (version 1.0)

Variance #: *To be filled in by the Computer Protection Program Manager (CPPM)*
Start Date:
Expiration Date: (Not to exceed two years)

1. Variance requestor: Jérôme Lauret

2. Required procedure for which you are seeking a variance.

A variance is requested for an alteration of several baseline policies and base control from “automation” to “manual” mode. Manual operations will be consistent with RHIC maintenance downtimes and respect basic CSPP policy scheduling. The area affected are:

- Automatic quarterly port & vulnerability scanning
- Automatic update
- Virus scanner

Additionally, we request the below feature to be disabled and hence, an exemption for the following

- Locked screens / screen saver

3. Device information (list information for each device: hostname, IP address, MAC address, OS, owner, system administrator, building, room)

This variance is submitted for the following nodes, all are described and covered by the SDAS (STAR Data Acquisition System) enclave document, part of BNL CSPP Research Enclave document section 4.2.11 and its addendum, “STAR-DAQ”. The list of systems is:

MAC	Host IP	Host Name	Owner
00010322C470	130.199.110.228	STAR-UTILITIES.STAR.BNL.GOV	Brown, Ralph
00104B308683	130.199.110.78	WELLES.STAR.BNL.GOV	De Phillips, Michael
0014223A7252	130.199.60.199	TPCGAS.STARP.BNL.GOV	Stringfellow, Blair
00104B2FE54A	130.199.60.202	DENEB.STARP.BNL.GOV	Betts, Wayne
00C04F991F4D	130.199.60.39	SHIFT-LEADER.STARP.BNL.GOV	Betts, Wayne
001676224E6B	130.199.60.41	TOFGAS.STARP.BNL.GOV	Schambach, Joachim
00C04F991E97	130.199.60.80	CHAPLIN.STARP.BNL.GOV	Stringfellow, Blair
001676A64691	130.199.60.82	BLANCHETT.STARP.BNL.GOV	Betts, Wayne
00C04F991F0C	130.199.60.83	ASTAIRE.STARP.BNL.GOV	Stringfellow, Blair
000103E0A89E	130.199.61.174	EMCSC.STARP.BNL.GOV	Betts, Wayne
000874358374	130.199.61.189	VIDEOPC.STARP.BNL.GOV	Lebedev, Alexei
00047630A4A1	130.199.60.15	PMDCS.STARP.BNL.	Betts, Wayne
08004616D32A	130.199.60.61	FTPCTEMP.STARP.BNL.	Betts, Wayne

4. Operation Affected by the Required Procedure: (Provide background for variance request; describe the devices, how they are affected by the required procedure, and why the required procedure cannot be met.)

This variance is requested for operational need purposes. All nodes are in need of the following alterations of the BNL baseline policy with explanation and mitigation herein provided:

- We would request to have all node exempt from automated quarterly (penetration) scanning during operation times to provide increased stability. Scanning has been demonstrated to significantly slow down the response time of those devices. However, note that such scanning would be made and requested manually during RHIC maintenance downtime periods consistent with quarterly scanning

OFFICIAL USE ONLY

Unclassified Computer Security Variance Request and Approval (version 1.0)

periods as well as BNL's scanning policy (only the automation is requested to be disabled).

- Automatic Update would be set to "download but do not install". This requires an alteration of the Windows XP guidance 4.1.2 "Automatic Updates". Automatic updates are often followed by a reboot which is incompatible with operation mode of constant experiment monitoring. Mitigation of the residual risk includes scheduled upgrade and reboot during RHIC maintenance downtimes. Each upgrade will be considered on a per schedule basis; maintenance schedules should allow for enough lead times to test the updates do not jeopardize operations of the monitoring nodes.
- We request an exemption of AntiVirus weekly (automated) scans. Anti-virus scans will be done on a manual basis. AntiVirus scans, causing a significant impact on performance (IO especially) overall could seriously hinder on operation and incapacitate the system requiring fast interactive response.

All manual operation will be performed by system administrators and contacts described the SDAS document section 1.6 (to the exception of the Information System PI, purely left in this section for administrative purpose).

The following feature is requested to be disabled:

- Nodes should be exempt of screen-saver locking mechanism. Screen savers would prevent operation requirements as all of the declared variance nodes do display monitoring information and visual alarms. Locked screen would hinder on the detection and view of those alarms hence, potentially causing harm to our experiment by the inability to catch them as early as possible.
- Mitigation
 1. All nodes are in visual contact of the experimental shift crew in the control room as described in SDAS document 2.1.2 "Physical Access" and section 3.1 (where physical access procedure is detailed).
 2. Accounts may be local group accounts with physical local access only or enclave network access through individually identifiable key exchange mechanism (double factor authentication) and consistent with SDAS section 3.1 "Access Control and Account Management" items AC-1 and AC-2.
 3. Mitigation for monitoring displays not immediately under visual proximity of the shift crew are controlled using an additional control mechanism: it includes the installation and use of the Rixler Computer Lockup (keyboard lock) software ; this software leave the screen unlocked but renders all keyboards or mouse interactions disabled apart from a "live" screen password unlocking dialog box. In practice, this solution provides the same access control philosophy than a screen-saver locked display ... with a visible display. The password in such case is separate from the group account and is known by the expert only.

5. Variance Approach: *(Analyze and describe how it will satisfy the intent of the required procedure.)*

Our request for a variance does not violate the philosophy of the baseline policy. Instead, it replaces automation by scheduled actions to best fit both operational needs and security needs. Screen saver locks are replaced by keyboard locks, keeping the need for constant monitoring possible while not impacting security access to computers not under direct supervision.

6. Required Actions: *(List actions to be taken based on the analysis of the approach in step 5.)*

All security measures proposed are currently in place and we have encountered no problems to date with those settings.

OFFICIAL USE ONLY

