Departmental Information Security Policy/Standard Waiver

Agency Name: _____ **Date**: 09/16/2009

Waiver Requester Name: Igor Filippov

Phone Number: 301-846-5961

Departmental Policy/Standard: FDCC

FIPS 199 Security Categorization of the Information System(s) For waivers covering multiple systems, provide the highest impact for each security objective:

Confidentiality: low Integrity: low Availability: low

Waiver Justification for Noncompliance or Deviation:

Explain why compliance with this policy/standard is not possible due to technical limitations, conflict with mission requirements, or other circumstances:

The computer systems for which this waiver is requested are being used to control scientific equipment. The vendors of the aforementioned equipment do not recommend significant deviations from the original configuration such as FDCC settings would mandate. The operation of this equipment is crucial to the mission of the Laboratory of Medicinal Chemistry. Property numbers: s053859, s067301, s058527, s062021, s063018.

Compensating Controls

Attach additional sheets if necessary to answer these questions. The relevant sections of the system security plan may be attached in lieu of re-entering the information here.

In the absence of the controls specified by this policy/standard, what compensating controls will be implemented and, if applicable, the control number from NIST SP 800-53:

The computer systems in question have been configured to obtain automatic updates on a weekly basis and run antivirus and anti-malware software. The user accounts controlling the instruments have been configured as limited user accounts. The computers are not being used as workstations or for casual web browsing.

Provide a justification for how the compensating controls provide an equivalent security capability or level of protection for the information system:

The compensating controls descibed above implement the most serious security recommendations of FDCC while still allowing to operate the scientific equipment.

Approval and Conditions

I, hereby, acknowledge that I have reviewed the aforementioned request for a policy/standard waiver and certify that the compensating controls necessary to justify the policy/standard waiver are adequate.

OPDIV, STAFFDIV, or Other Approved HHS Security Representative Signature[1]	Date

Upon approval, submit a copy of this waiver to SecureOne via fax (202-690-8715) or scan and e-mail to SecureOne.HHS@hhs.gov. The approver shall retain the original.

Please note: This policy/standard waiver supersedes the policy waiver previously included within the *Secure One HHS Information Security Program Policy*. This waiver and its applicability must be reviewed at least annually by the requesting OPDIV. Waivers must be renewed every three years or when significant changes which affect the system categorization, justification for noncompliance and/or compensating controls are made.

[1] In most cases the OPDIV-level Chief Information Security Officer (CISO) will be the appropriate approver unless otherwise noted in the individual policy or standard for which the waiver is submitted. This includes but is not limited to the *Department of Health and Human Services (HHS) Encryption Standard.*