Network Security Activities Under the University's Electronic Communications Policy

This guidance is intended to assist the Campuses and Laboratories in undertaking additional network security efforts. This guidance specifically addresses how the University's Electronic Communications Policy (ECP) applies to network security activities. Because technology develops so much more rapidly than policy, this guidance is limited to describing the basic principles of the ECP and how they apply to general categories of network security activities. For more specific advice with respect to a particular network security technique or functionality, Campuses and Laboratories are encouraged to consult with their respective Cyber-Risk Responsible Executive and/or the Office of General Counsel.

I. General Rule: Access to Electronic Communications Requires Consent

The ECP establishes the following general rule: "An electronic communications holder's consent shall be obtained by the University prior to any access for the purpose of examination or disclosure of the contents of University electronic communications records in the holder's possession." This basic rule establishes the default expectation of informational privacy for authorized users of the University's electronic information systems.

II. Exceptions to the General Rule: System Monitoring and Security Practices

The ECP expressly authorizes network security activities, including inspection of network traffic for security purposes:

> University employees who operate and support electronic communications resources *regularly monitor transmissions for the purpose of ensuring reliability and security of University electronic communications resources and services* (see Section V.B, Security Practices), and in that process *might observe certain transactional information or the contents of electronic communications.* Except as provided elsewhere in this Policy or by law, they are not permitted to seek out transactional information or contents when not germane to system operations and support, or to disclose or otherwise use what they have observed. In the process of such monitoring, any unavoidable examination of electronic communications (including transactional information) *shall be limited to the least invasive degree of inspection required to perform such duties.*

(ECP, Section IV.C.2.b (emphasis added).)

The System Monitoring authorization is supported by an additional provision of the ECP that includes express authorization for "Security Practices":

> Providers of electronic communications services ensure the integrity and reliability of systems under their control through

> the use of *various techniques* that include routine monitoring of electronic communications. *Network traffic may be inspected to confirm malicious or unauthorized activity that may harm the campus network or devices connected to the network. Such activity shall be limited to the least perusal of contents required to resolve the situation. User consent is not required for these routine monitoring practices.* Providers shall document and make available to their users general information about these monitoring practices. If providers determine that it is necessary to examine suspect electronic communications records beyond routine practices, the user's consent shall be sought. If circumstances prevent prior consent, notification procedures described in Section IV.B.3, Notification shall be followed.

(ECP, Section V.B).

Like the "System Monitoring" provision, the "Security Practices" provision contemplates that network security monitoring may include access to contents of communications, following the "least perusal" principle.

This provision also requires that general information should be made available to users about the University's network security practices. This does not require the dissemination of technical details or specific functionalities. The purpose of this provision is to provide "general" information about such activities, in clear terms that are understandable to users who may not have technical expertise.

a. Use of Automated Systems for Network Security

The ECP's Implementation Guidelines explicitly provide that "automated inspection of electronic communications in order to protect the integrity and reliability of University electronic communications resources does not constitute nonconsensual access." (ECP, Implementation Guidelines Section III.B.4.) Some basic network security tools, such as intrusion detection systems, use automated technical features to identify potentially malicious activity on a campus or location's network. The ECP specifically exempts such automated inspection techniques from the consent requirement to protect the integrity and reliability of the University's systems.

III. Limits on System Monitoring and Security Practices

The ECP permits review of both the transactional elements and the content of electronic communications to respond to a network security threat. To protect the privacy of users, the ECP also imposes important limitations on such review.

a. "Least Perusal" Standard

Network Security Activities Under the University's Electronic Communications Policy

The inspection of network traffic for security purposes must be limited to "least perusal of contents required to resolve the situation." (ECP, IV.C.2.b & V.B.) This means, for example, that a Campus or Laboratory should attempt to resolve a security concern by review of transactional data at first, without review of the human readable content of an underlying electronic communication.

In circumstances where a security threat cannot be resolved at a lower tier (or, indeed, where security concerns are *amplified* by such review of transactional data), the human-readable content of an underlying communication may be reviewed. In such cases, the ECP limits such inspection to the "least perusal" of content necessary to resolve the concern. To inspect content further than is permitted for routine network security purposes, the ECP requires user consent, or access without consent under a campus's procedures, which typically involves approval by Campus or Laboratory's upper management, as discussed below.

b. Restrictions on Use of Network Security Data

The ECP forbids the University from using network security data for non-security purposes, (ECP, II.E.2, IV.A, & IV.C.2.b (prohibiting University employees from seeking out, using, or disclosing personal data observed in the course of performing university network security duties)), and violators are subject to discipline. The ECP does create a specific exception for circumstances where an employee incidentally observes obvious illegal activity in the course of performing routine network security activities. (ECP, IV.C.2.b (defining exception for disclosure of incidentally viewed evidence of illegal conduct or improper governmental activity).)

With respect to storage, much data analyzed through network analysis may already be stored elsewhere within the University's network ecosystem (or even with third party cloud or other providers), independent of any network analysis activity. Data analyzed or aggregated specifically for network security purposes should only be stored for a limited time, segregated from other network resources in a highly secure system, and forensically obliterated thereafter. In some circumstances, a preservation of certain data related, for example, to anticipated litigation or a regulatory investigation, may be required by law, which may result in a longer storage period for a limited amount of network analysis data subject to such a mandate. With respect to third party requests for such data, the University should carefully scrutinize such requests, from whatever source, to ensure that user privacy expectations are protected.

c. Vendors and Contractors Performing Network Security Activities

For vendors who assist with network security activities, the ECP requires them to be contractually bound to honor University policy, including the ECP. (*See* ECP, IV.A.) It is also recommended that, even in otherwise time-sensitive circumstances, privacy impacts should

be evaluated before undertaking a coordinated network security effort. Appropriate privacy protection measures should be embedded, as feasible, into the underlying scope of work both at the planning and execution stages of a network security project. Such analysis typically should include an evaluation of the specific technical and analytic techniques to be used and whether they are consistent with the ECP. Campus and Laboratory security and IT teams may properly consult with their respective privacy officials and the Office of General Counsel to assist with such analysis, including defining an appropriately limited scope for network analysis activity. To further ensure adherence to University policy, it is recommended that vendors agree to follow the ECP and the University's standard terms and conditions related to data security, currently contained in Appendix DS.

IV. Access Without Consent (AWOC)

In addition to the broad exception to the consent requirement for network monitoring and security practices, additional exceptions provide for review of the content of electronic communications: when required by law, when there is substantiated reason to believe violations of law or certain University policies have taken place, when there are compelling circumstances, and under time dependent, critical operational circumstances. Where one of these exceptions apply, the policy authorizes the University to obtain authorization to review from an official designated by campus policy under the "Access Without Consent" or "AWOC" provisions of the ECP and may require notice to an affected individual rather than consent. (ECP Section IV.B.) Each campus has designated an approving official at a senior level.

###