

**OLD DOMINION UNIVERSITY**  
**University Policies and Procedures**

**3503 - COMPUTER SECURITY REGULATIONS**

Statement: All users of the University's computing resources have the responsibility to report known or suspected violations of the security regulations.

The University Data Security Administrator should be informed of any suspected violation, and may assist in the investigation and provide appropriate documentation, when requested. When not directly involved, the Security Administrator should also be informed of the final disposition in a timely manner. The Security Administrator also acts as the contact person, and coordinates communications with outsiders.

The Internal Auditor may be asked, depending upon the severity of the suspected violation, to serve as the central coordinator of a formal investigation. A representative of Public Safety may also be involved in the investigation.

Both the Vice President for Administration and Finance and the Vice President of the area investigated will receive the report resulting from any formal investigation conducted by the Internal Auditor.

The Vice President for Administration and Finance is the final authority on matters pertaining to suspected abuse.

Reported violations of the security regulations will be investigated as they occur and will be concluded in a timely manner. Unless there are extenuating circumstances, the time from the initial report of a suspected violation to the investigation's conclusion will not exceed ten working days. If necessary, the system administrator may take operational steps to immediately safeguard resources by prohibiting access to the systems by those suspected of violating ethical use guidelines and policies. This would be done only when there is evidence of a clear threat to those resources. If the system administrator declines to take these steps, a higher authority may then override this decision, and require that it be done.

If necessary, the University reserves the right to inspect the contents of files and any related computer-generated or stored material, such as printouts. Unless notification would compromise the investigation, the user should be notified prior to the inspection. The Vice President for Finance and Administration or an authorized representative must be convinced of sufficient cause before it can be done without the user's permission.

## **Reporting and Investigation**

The nature, severity, and possible consequences resulting from violations cover a wide spectrum. The investigative procedures, and resulting punitive measures, as well as the time elapsed, should be reflective of this difference.

Very minor violations should be reported to and may be totally handled by the Data Security Administrator or designee. The relevant system administrator should also be notified, and, in some cases, may provide additional investigative information. Usually, a warning communicated to the offender will suffice. To be handled in this manner, the violation must not involve any threat to the integrity and operation of the system/network. Examples of violations that could be considered in this category are distribution of chain letters, and a single and minor instance of harassment.

These violations should be dealt with quickly; resolution should not take longer than two working days at the maximum.

When a more serious violation is suspected, it should be reported to the relevant system administrator and the Data Security Administrator as soon as possible. If the notification comes from an external source, the message should be forwarded to the relevant system administrator. If more than one system could be involved, each system administrator must be notified.

The system administrator(s), Data Security Administrator and/or other appropriate staff will conduct a brief initial investigation to gauge the seriousness of the violation, and its effect, if any, on the system/network.

## **Incidents Involving Students:**

The Data Security Administrator and the relevant system administrator(s) will work together in the investigation. Based upon their findings, the Data Security Administrator will write up a report, complete with all supporting documentation. This will be sent (via confidential campus mail) to the University Hearing Officer in Student Services. Copies of the report should be sent to any other relevant parties.

Student Services will then take the appropriate measures to address the suspected violation. The Data Security Administrator and any other relevant parties may be further consulted by Student Services, and may additionally be required to participate in a hearing or other meeting.

Upon the completion of this process, Student Services shall formally report the results of their investigation and the resulting action(s) to the Data Security Administrator and the Dean of the student's degree area, if appropriate.

## **Incidents Involving Faculty, Staff, and Non-Old Dominion Parties:**

Depending upon the seriousness of the infraction, the following procedures should be followed.

### **Informal Investigation:**

If the system administrator feels the incident is minor and would be best handled informally within the department, that recommendation should be made to the Data Security Administrator (DSA). If the DSA is in agreement (the Internal Auditor may be consulted, if necessary), the investigation may then be conducted by the administrator, or one designated by the administrator. The administrator is expected to include any other people whose involvement is necessary for a full investigation. Additionally, the Data Security Administrator should be kept informed of the progress of the investigation, and, at its conclusion, the actions taken by the department.

Investigations should be completed in a timely manner. Unless there are extenuating circumstances, the elapsed time should at no time exceed ten working days.

### **Formal Investigation:**

If the violation is deemed serious by both the system administrator and the Data Security Administrator, a more formal investigation is indicated. In cases where the system administrator and Data Security Administrator disagree, the Vice President for Administration and Finance will be the final authority. The advice of the Internal Auditor and other system administrators may be solicited to aid in this decision.

Once the decision has been made to conduct a formal investigation, the Data Security Administrator will make the request to the Internal Auditor. This must be a formal written request, with copies going to the Vice President of Administration and Finance as well as the Vice President of the area to be investigated. If the Auditor agrees to conduct a formal investigation, the procedures below are to be followed:

The Internal Auditor will serve as the central coordinator for the investigation.

The investigation team will consist of the Internal Auditor, the Data Security Administrator, and the relevant system administrator(s). Others, such as a representative from Public Safety or departmental computer contacts, may be asked to participate by the Internal Auditor.

As spokesman for the team, the Internal Auditor may request that information be provided by others with knowledge relevant to the incident; it is imperative that the requested information be provided within the Internal Auditor's stated time frame. If the team feels it is necessary, others may also be interviewed as part of the investigative process.

The investigation team, once all information is gathered, will decide what actions, if any, it feels should be taken. A report will be written by the Internal Auditor, based upon the findings of the team, and will detail the violation(s), the results of the investigation, and recommended actions. Copies of this report will be delivered to the Vice President for Administration and Finance and the Vice President of the area investigated.

Unless there are extenuating circumstances, the investigation should be completed within ten working days from when the violation was reported to the Internal Auditor.

Upon receiving the report, the Vice President(s) will decide what action(s) should be taken, if any, and relay this information to the Internal Auditor and the Data Security Administrator.

### **Computer Incidents Involving External Sites**

Computer system security incidents do not obey network, national, or architectural boundaries. Effective computer security incident response, therefore, requires communication and coordination across multiple communities.

Old Dominion University not only has an obligation, but also a vested interest in responding quickly and effectively to incidents originating on campus as well as reports and advisories received from external sources. These external sources may also include alert lists such as CERT, ISS, and VA-CIRT.

The Data Security Administrator will act as the point of contact for all such security incidents. All incoming reports/notifications should be forwarded to the DSA, and all responses to external contacts/agencies will be coordinated through the DSA.

System administrators are expected to evaluate the applicability of advisories to their systems and take whatever action is appropriate. If a local security incident appears to have significance for other sites, the appropriate external list(s) and/or agencies will be notified by the DSA in a timely manner.

Those needing to report an incident should send email to [abuse@odu.edu](mailto:abuse@odu.edu).

**Responsibility:** Vice President for Administration and Finance

**Authorization:** James V. Koch, President

**Date:** December 1, 1988; Revised July 1, 2000

**Effective Date:** July 1, 2000