## Appendix E:
## Crisis Procedure – Information Security

### Decision-Making Process

If an information security issue (network security breach, personal data loss, ransomware attack, etc.) is anticipated or has occurred on the Corvallis campus, OSU's Executive Leadership and Office of Information Security staff will meet to assess the situation and decide on a course of action.

Additional consultation may involve the affected system owner, contractor support or Administrators at other OSU locations, such as Cascades, Hatfield Marine Science Center, the Portland Center and Extension Offices/Experiment Stations.

### Communication Release Approval Process

A decision to conduct internal and/or external communication will be made and communicated to appropriate audiences as soon as possible, using an approved message tailored for different communication channels.

The message will be originated by University Relations and Marketing and approved by members of the leadership team.

| Topic | Subject Matter Expert |
|---|---|
| • Compromise of personal information<br>• Compromise of student information<br>• Compromise of Research information<br>• Compromise of OSU information technology systems | • VP UIT/CIO<br>• VP Academic Affairs<br>• VP Research<br>• VP UIT/CIO |

### Communicating the Impact on Operations

Information about details or impacts of the Information Technology issue may be shared with the news media by News and Research Communications.

Other information distribution will be determined by the VP UIT/CIO, with consultation of University Relations and Marketing.

### Follow-Up Communications

Updated decisions or information will follow the same decision-making protocol and communication process listed above until the incident has ended and normal operations resume.