and Warning Notification to Administrator", "E. Responding to the National Institute of Informatics Information Security Operation Collaboration Service (NII—SOCS)", "F. Operational support for IT asset management systems" and "G. Other security-related operations".

③ Provision of information

The Contractor shall check the latest security information issued by public security organizations such as IPA, JPCERT／CC (Japan Computer Emergency Response Team Coordination Center) on a daily basis, collect and organize information deemed necessary by the University, and provide it by e-mail. As a general rule, the information will be provided only to the distribution address designated by the University. In principle, delivery is based on once every two weeks. However, if the amount is urgent, it will be delivered immediately. In doing so, keep in mind that the recipient can immediately recognize that it is urgent. Regarding the software to be used for the form to be provided, the university must discuss with the university in advance and prepare and provide the distribution document.

④ Security business support

In consultation with the staff in charge of the University, engineers with technical skills equivalent to those of security consultants shall provide 120 hours of operational support per year within the contract period. The main business support contents are as follows.

A Information security lecture instructor and preparation of training materials

B Preparation and update of information security materials

C Field surveys, user support, witnessing planned power outages and network configuration changes, etc.

⑤ Implementation of information security audits

Based on the Niigata University Information Security Policy, conduct advisory-type audits by extracting audit items that match the actual situation of the University. Specifically, items for auditing the status of business operations in accordance with the procedure manual should be extracted, and audited from a professional perspective to ensure that information assets handled in business are properly operated and managed through questionnaires, interviews, on-site inspections, etc.

⑥ Implementation of targeted e-mail attack drills

To send e-mails simulating targeted attack e-mails to e-mail users of the University, and to conduct training and post-training education on targeted attack e-mails.

⑦ Implementation of vulnerability assessments

Use the vulnerability assessment tool (nessus) provided by the University to diagnose vulnerabilities in devices connected to the University network. If the diagnosis results indicate a vulnerability with a high degree of urgency, notify the device manager of the improvement.

⑧ Implementation of ASM Assessment

Using a cloud-based ASM tool provided by the contractor, assess the vulnerabilities of equipment exposed to the external network by the university. For vulnerabilities deemed high-priority, notify the equipment administrators of the need for corrective action.

⑨ IT Asset Management Tool Operation Support

Using the IT asset management tool provided by the university (Tanium, Inc.), provide the following operational support :

A Use the vulnerability assessment function to conduct vulnerability assessments on endpoints and notify the administrators of equipment deemed high-priority of the need for corrective action.

B Use the function to detect suspicious activity on endpoints and notify the equipment administrators of any deemed high-priority issues of the need for corrective action.

⑩ Other Notices

A Hold regular meetings at least once a month to discuss operational procedures, etc. with the person in charge of the University.

B Operational procedures, etc. discussed at regular meetings, etc. shall be recorded in writing (including electronic media).

C If a security consultant is to be changed within the contract period, an appropriate period shall be established for the transfer of operational procedures, etc., and the details shall be reported to the staff in charge of the University for Confirmation.

D Upon expiration or termination of this Agreement, all necessary data assets and operating procedures shall be provided in electronic form in consultation with the University. In addition, the latest data assets at that time must be provided as electronic media at least three months in advance.

E Upon expiration or termination of this Agreement, close meetings shall be held with the University and the new contractor.

F Remote work shall be carried out with the permission of the University via VPN connection.

G When working remotely, the work terminal shall not be used for any purpose other than the University's information security support work. In addition, work terminals should take sufficient security measures against information leakage, including the installation of anti-malware software.

H You must not take out the University's information data, including maintenance data. However, this excludes cases in which the contents of the take-out, how to handle it, and the security measures thereof have been discussed with the faculty and staff in charge of security at regular meetings, etc., and permission has been obtained from the director of the Information Technology Center of the University. In addition, when actually taking out information data with the prior permission of the Director of the Information Technology Center, prepare two copies of the information data transfer form (one for university storage and one for storage by the contractor) and submit it to the faculty and staff in charge of security at the University. The removal of information data that is not recorded in this transfer form shall be deemed to be the removal of information data without the permission of the University.

I At the regular meeting, submit a list of work history (work content, worker, work date and time, work terminal, etc.).

(5) Time limit for the submission of the requested material : 17 : 00, 8 June 2026

(6) Contact point for the notice : Miki Suzuki, Financial Management section, Niigata University, 8050 Ikarashi 2-no-cho Nishi-ku Niigata-shi 950—2181 Japan, TEL 025—262—7674