Botany IT Security Alert Guideline

An IT security alert is an IT-related security warning that needs to be sent to a target group so that people may take any necessary actions to protect their IT devices from threats that may possibly affect large numbers of Botany department members. Due to the nature of IT security threats, an IT security alert is highly time sensitive and must be delivered to the target group as quickly as possible.

1. Botany IT is the only authorized unit that can initialize an IT security alert. Anyone outside the Botany IT unit is encouraged to send IT security information, including concerns and IT security warnings from external sources, to Botany IT helpdesk. Botany IT staff will then verify the information and assess the threat before forwarding a formal alert to the target group within Botany.
2. Within Botany IT, any Botany IT staff is encouraged to initiate an IT security alert once he has learned of a security problem through any resource. The initial draft alert should include:
    a. A brief description of the security problem;
    b. the scope of the affected users, software, and/or devices;
    c. preventative tips and suggested actions to be taken;
    d. the source of the information;
    e. URL(s) to external resources that provide further details on the threat.

    The initial draft alert should be sent to all Botany IT staff by email.
3. Within the Botany IT unit, the senior member on duty should decide within fifteen minutes of the initial draft alert issuance whether a formal alert should be issued to external groups. If the senior member on duty decides that an alert should not be sent to external groups, he must reply to the person who drafted the alert with a brief rationale for the decision, and cc this message to all Botany IT staff. Otherwise, he must forward the draft alert (or a revised version) to all three office staff members (Isabel, Veronica, and Jessica, in case one of them is off duty) within 30 minutes after the initial draft alert was sent out, while clearly indicating which target group the alert should be sent to (for example, faculty group, student group, staff group, or everyone). In the meantime, the senior IT staff member on duty should cc the email to all other IT staffs.
4. The three office staff members (Isabel, Veronica and Jessica) are responsible for communicating with each other so that no duplicate emails are sent to the target group(s). The primary contact is Isabel, but in her absence, Veronica should send, and finally Jessica.
5. If the IT staff who drafts the initial alert is the senior member on duty, he can forward the alert to the three office staff directly, and cc all other IT staff.
6. If the IT staff who drafts the initial alert receives no response from the senior IT staff on duty one hour after having sent it to all IT staff, he is encouraged to forward his draft alert to all three office staff, while clearly indicating the target group(s).