

**Kiosk Announcements**

- By Date
- By Region
- By Topic
- By VPU

**Events**

**What's New**

**Senior Staff Appointments**

**B-Span**

**Add New**

**My Kiosks**

**Site Tools**

- How to post
- Kiosk Policies/FAQ
- Event Publishing Guidelines
- Archives

## August 19 Update on Information Security

**Date:** August 19, 2008 - 04:16

**Sponsor:** Information Solutions Group

Note: IFC's information security policies are governed separately and IFC users are not affected.

The [Information Security Council \(ISC\)](#) which governs information security risk management has been provided with a confidential risk assessment presented by the [Office of Information Security](#) and has discussed the longer term response. In addition to the actions previously endorsed to strengthen controls both inside the network and at the information security perimeter, the ISC has made the following **decisions**:

- Implement a stronger method of authenticating users when they access the Bank's network and applications from both inside and outside the Bank and to implement it as soon as possible. This will likely require staff to carry a small device or card with them (like the SecurID now required for remote access to webmail) and use it in combination with a password. Ideally, in the medium-term the objective ISC has set is to have one method with one password for logging into the network whether from the office, home, or travelling using a Bank PC or a non-Bank PC.
- The deadline for all Bank staff to take the [online information security awareness course](#) is brought forward to December 31, 2008. This measure has been taken to ensure that staff members are aware of the kinds of attempts which may be made to capture their passwords through fake email and other scams. Please do not open an email attachment or click on an internet link unless you are certain that it is from a trusted source.
- In the interim, until a stronger method for secure access is implemented, the current practice of allowing staff to use the same password for all their password-protected applications will be suspended, and the Password Plus website will be disabled. In addition, all passwords will be expired every 90 days and the complexity of passwords will be increased.
- Staff will be notified by email when it is time to reset their passwords in the next few weeks. The specifics of these password changes will be communicated and coordinated by local VPU and ISG IT teams. Passwords will be changed on a rolling basis and the process will be managed by local VPU IT teams who will be available to assist staff. **You will be notified by an email from the account 'ISG Password Change Notification' with instructions when it is time for you to change your passwords.**

As reported in the Information Security updates on July 18 and August 6, an external attempt was made to compromise the Bank's information network. Consistent with our procedures, several actions have been taken to counter this threat, and confidential briefings have been provided to appropriate groups within the Bank. Actions most visible to end-users have been (a) tightened controls on external websites, (b) resetting of passwords, and (c) deployment of SecurID for webmail access. As previously reported in mid-July, we would like to reassure you that there is no evidence that Bank staff personal information is at risk from the recent external attempts. We appreciate that staff have already changed their passwords once, and this has strengthened security. However, to continue to strengthen our security controls, the additional actions noted above are now being taken.

Information security is a continuous process of identifying and responding to new risks and balancing competing business needs. We ask for your patience and will continue to provide updates on this security incident.

Co-Chairs of the Information Security Council

Diann Dodd Martin  
Director, TRODR

Guy-Pierre De Poerck  
VP and CIO, ISGVP

**For Information:** ISG Global Support Center

**Please rate this page !**

LOW HIGH

Average : ★★★★★ (192 votes)

[▲ Top](#)

Permanent URL for this page: <http://go.worldbank.org/IDLS1NABYO>