

Department of Fish and Game

DIRECTOR'S BULLETIN

No. 2008-02

To: All Department Staff Date: June 9, 2008
From: Donald Koch
Director
Subject: Policy for Protecting the Confidentiality of Personal Data

Security has always been an essential component of information privacy at the Department of Fish and Game (DFG). Implementing an effective information security program is essential for DFG to fulfill its responsibilities towards the individuals who entrust us with their personal, sensitive and confidential information.

To effectively implement an information security program, it is necessary for DFG programs that collect or manage individuals' personal, sensitive and confidential information, to use reliable safeguards to protect that information against unauthorized access or disclosure. To assist DFG Programs in protecting this information, whether it pertains to customers, employees or others, DFG has created a *Policy for Protecting the Confidentiality of Personal Data*. This policy is located on the Office of Training and Development's Intranet homepage under the Mandated Training link or http://dfgintranet/Portal/Portals/0/OTD/policy_for_protecting_confidentiality_of_personal_data.pdf

This policy is consistent with "best practices" that have been implemented for private businesses and other organizations to manage personal, sensitive and confidential information in ways that promote and protect individual privacy interests. The new policy requires the following actions:

1. DFG program managers/supervisors must provide ongoing awareness for all employees, contractors and business partners, who handle personal, sensitive and confidential information, to follow security and privacy policies, and to recognize and report a potential breach.
2. DFG employees who handle personal, sensitive and confidential information must **annually review** this policy and **sign the Privacy Protection Acknowledgment form** at the end of the document.
3. DFG managers/supervisors must provide this policy to new employees as part of the employee orientation process.

The DFG's Chief Auditor has been designated as the Information Security Officer (ISO) and is responsible for monitoring compliance with this policy. Any violation of this policy must be reported immediately to the DFG's Chief Auditor, Brian Kwake, at (916) 445-3780 or BKwake@dfg.ca.gov.