

DATA BREACH MANAGEMENT & RESPONSE PLAN



PURPOSE

This plan outlines the steps to follow in the event of an imminent or actual breach of personally identifiable information (PII) and identifies and describes the roles and responsibilities of the *Boys & Girls Club of Greater Ventura* Data Breach Response Team (DBRT or “Team”).

DEFINITIONS

For the purposes of this plan, a **breach** refers to the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an *authorized* user accesses or potentially accesses personally identifiable information for a purpose that is not authorized. A breach can lead to an adverse impact on information assets such as an information system and/or network and mobile devices.

The following pages describe breach severity levels, responsibilities of the Boys & Girls Club of Greater Ventura Data Breach Response Team, and a communication plan.

In the event of a breach, **one of the first steps** the designated DBRT lead should take is to:

1. Report an actual or detection of an imminent breach of PII to Boys & Girls Clubs of America (BGCA) via the BGCA CIMS (Club Incident Management System) **no later than 12 hours after an occurrence of an actual breach or detection of an imminent breach**.
2. Agree to free exchange of information with representatives of the U.S. Department of Justice, Office of Justice Programs, as needed.

Outages caused by scheduled maintenance, or authorized, planned activities that cause expected outages as part of those activities are not included in this definition and for the purpose of this plan. Examples of information security incidents may include (but are not limited to):

- Unauthorized access or use of a system
- Unauthorized use of the system as a gateway to other systems
- Unauthorized use of any account
- Compromise of “restricted”, “confidential”, non-public information
- Execution of malicious code that destroys data
- Computer security intrusion (physical)
- Unauthorized change to computer or software
- Loss or theft of equipment used to store private or potentially sensitive information
- Denial of service attack
- Interference with the intended use of an information technology resource
- Insider Sabotage
- Mishandling of Information / Data Assets



DATA BREACH MANAGEMENT & RESPONSE PLAN (con't.)

SEVERITY LEVELS

All actual breach events detected will be categorized according to one of the following four (4) severity levels:

1. Critical
2. High
3. Medium
4. Low

The severity levels have been set based on the impact of the incident to the **Boys & Girls Club of Greater Ventura**.

Severity Level	Exposure	Description
Level 1 - Critical	Public Facing Incident <i>(A breach that is visible to the general public and/or has implications for the Club's brand, whereby the breach could erode customer confidence.)</i>	A direct and significant threat to the brand of Boys & Girls Club of Greater Ventura. Some financial loss is likely in such incidents and customer impact may be widespread. Such incidents could involve loss of sensitive data, total loss of a crucial service or business function; severe degradation of critical system performance. Generally involves escalation to senior management at Boys & Girls Club of Greater Ventura. Examples include: • Large scale disclosure of the personally identifiable information of members or staff of Boys & Girls Club of Greater Ventura. • Large scale attack on the Club's systems, or on third-party hosted information assets causing a virtual lockdown of all online services. • Malware or Ransomware attack affecting virtually all of the information assets of the Boys & Girls Club of Greater Ventura. • Multiple customer / cardholder data compromised



DATA BREACH MANAGEMENT & RESPONSE PLAN (con't.)

Severity Level	Exposure	Description
Level 2 – High	Internal - Club Facing Incident <i>(An incident that does not involve external parties, and is not publicly known, but is propagated throughout the Boys & Girls Club of Greater Ventura.</i>	May involve limited disruption to the Club and impact with potentially repeated errors or possibility of reoccurring attacks against information assets. These incidents may involve non mission-critical business applications and systems Examples include: • Unauthorized access to a non-privileged account on a non-mission critical system or application. • A limited number of end user workstations affected by known malware. • Multiple customer / cardholder data compromised
Level 3 – Medium	Internal to the Boys & Girls Club of Greater Ventura	May involve a potential (but unrealized) threat to the Club's information assets. In some cases irregular but unconfirmed security breaches may be classified under this level. The impacted system(s) usually are not expected to have a significant business impact. Examples include: • Multiple internal systems affected by a virus. • An internal file server is compromised by a disgruntled employee. • Inappropriate material is distributed internally via e-mail.
Level 4 – Low	Internal to Boys & Girls Club of Greater Ventura	A system is compromised without access to sensitive data. Examples include: • A single workstation infected with a known form of malware (a virus with a confirmed signature). • Unsuccessful attempt to port scan a target system from an unknown external source.

Other adverse events include floods, fires, electrical outages and excessive heat that cause system crashes. Adverse events such as natural disasters and power-related disruptions are not generally within the scope of this Data Breach Management & Response Plan.



DATA BREACH MANAGEMENT & RESPONSE PLAN (con't.)

DATA BREACH RESPONSE TEAM (DBRT)

A DBRT is established to provide a quick, effective and orderly response to a breach of PII and other related incidents such as virus infections, hacking attempts and break-ins, improper disclosure of confidential information to others, system service interruptions, and other events with serious information security implications.

The DBRT's mission is to prevent any loss of PII, other sensitive or confidential information, or public confidence by providing an immediate, effective and skillful response to any unexpected breach involving computer information systems, networks or databases.

DBRT MEMBERS

Each of the following members will have a primary role in incident response:

- ☐ CEO
- ☐ Board President

Each of the following members may provide supporting roles during incident response. Additional personnel may be identified to participate as appropriate:

- ☐ Director of Operations
- ☐ Board Safety Chair

DBRT ROLES AND RESPONSIBILITIES

DBRT Team Lead - Breach Oversight and Communication Protocol

- ☐ Report actual or imminent breach of PII to Boys & Girls Clubs of America (BGCA) via the BGCA CIMS (Club Incident Management System) **no later than 12 hours** after an occurrence of an actual breach or the detection of an imminent breach. BGCA is required to notify the U.S. Department of Justice within 24 hours of breach detection.
- ☐ Declares an Information Security incident exists.
- ☐ Determines the nature and scope of the incident.
- ☐ Contacts qualified information security specialists as needed.
- ☐ Acts as central point of contact for an incident.
- ☐ Contacts members of the DBRT.
- ☐ Communicates with executive leadership as appropriate.
- ☐ Determines which DBRT members play an active role in the investigation.
- ☐ Provides proper training on incident handling.
- ☐ Escalates to executive management as appropriate.
- ☐ Monitors progress of the investigation.
- ☐ Ensures evidence gathering, chain of custody and preservation is appropriate.
- ☐ Prepares a written summary of the incident and corrective action taken for distribution to executive leadership.
- ☐ Assesses the execution of the Data Breach Management & Response Plan.



DATA BREACH MANAGEMENT & RESPONSE PLAN (con't.)

IT Manager or Managed Service Provider - Information Technology Systems Oversight and Monitoring

- ☐ Oversees all IT related activities.
- ☐ Assesses and advises on issues related to IT and to communications and network systems such as telephones, servers, computers, etc.
- ☐ Coordinates all emergency telephone service as needed.
- ☐ Monitors critical applications and processes.
- ☐ Coordinates and ensures critical processes and application are operating as needed.
- ☐ Analyzes network traffic for signs of denial of service, distributed denial of service, or any other attacks.
- ☐ Coordinates the execution of any tracing tools such as sniffers, Transmission Control Protocol (TCP) port monitors and event loggers.
- ☐ Looks for signs of a firewall breach.
- ☐ Contacts external internet service provider for assistance in handling the incident.
- ☐ Takes action necessary to block traffic from suspected intruder.
- ☐ Ensures all service packs and patches are current on mission-critical computers and critical file shares.
- ☐ Ensures backups are in place for all critical systems and critical file shares.
- ☐ Monitors business applications and services for signs of attack.
- ☐ Reviews audit logs of mission-critical servers for signs of suspicious activity.
- ☐ Ensures database backups are in place for all critical systems.
- ☐ Examines database system logs of critical systems for unusual activity.
- ☐ Monitors the physical security of and access to equipment.
- ☐ Provide support to all Club personnel during the incident.
- ☐ Central point of contact for all technology support issues and questions.

CEO - External Communication

- ☐ Coordinates public information and media relations pertinent to the incident or emergency situation.
- ☐ Communicates factual information to the news media, public, and employees.
- ☐ Receives and processes all inquiries from external sources.
- ☐ Corrects misinformation or rumors and disseminates factual information to media sources.

Club Attorney - Legal and Human Resources

- ☐ Determines and coordinates any legal impact and correspondence.
- ☐ Provides input to the DBRT on legal matters.
- ☐ Determines and coordinates disciplinary effort if an employee is suspected of causing an incident.
- ☐ Assesses the impact of the situation on employees.
- ☐ Provides support for human resource elements of recovery and employee notification.
- ☐ Coordinates operations and personnel needs.



DATA BREACH MANAGEMENT & RESPONSE PLAN (con't.)

COMMUNICATION PLAN

Upon activation of the DBRT, it is the responsibility of the CEO to facilitate communication and to closely manage and control the notification process.

The Club CEO is responsible for establishing guidelines and procedures for external communications related to a breach. No Club staff member, except the designated spokesperson has authority to discuss any breach with any person outside of Boys & Girls Club of Greater Ventura. Unauthorized disclosure of a breach could lead to greater disruption and financial loss than the incident itself.

PRIMARY CONTACT INFORMATION

CEO

Patti Birmingham
(805) 641-5585 Office
(805) 207-3531 Mobile
pattib@bgclubventura.org

Director of Operations

Simon Salem
(805) 641-5585 Office
(805) 766-5003 Mobile
simons@bgclubventura.org

Board Safety Chair

Peter Barry
(925) 324-4916 Mobile
peterb@advantagetelnet.com

IT Manager or Managed Service Provider

ACM Computers
(805) 650-6728 Office
servicedesk@acmit.net

Local Law Enforcement – Police Department (LeFevre, Westview & Org-wide Event)

(805) 339-4400 Office

Local Law Enforcement – Sheriff Department (Oak View & Harrison)

(805) 654-2380 Office