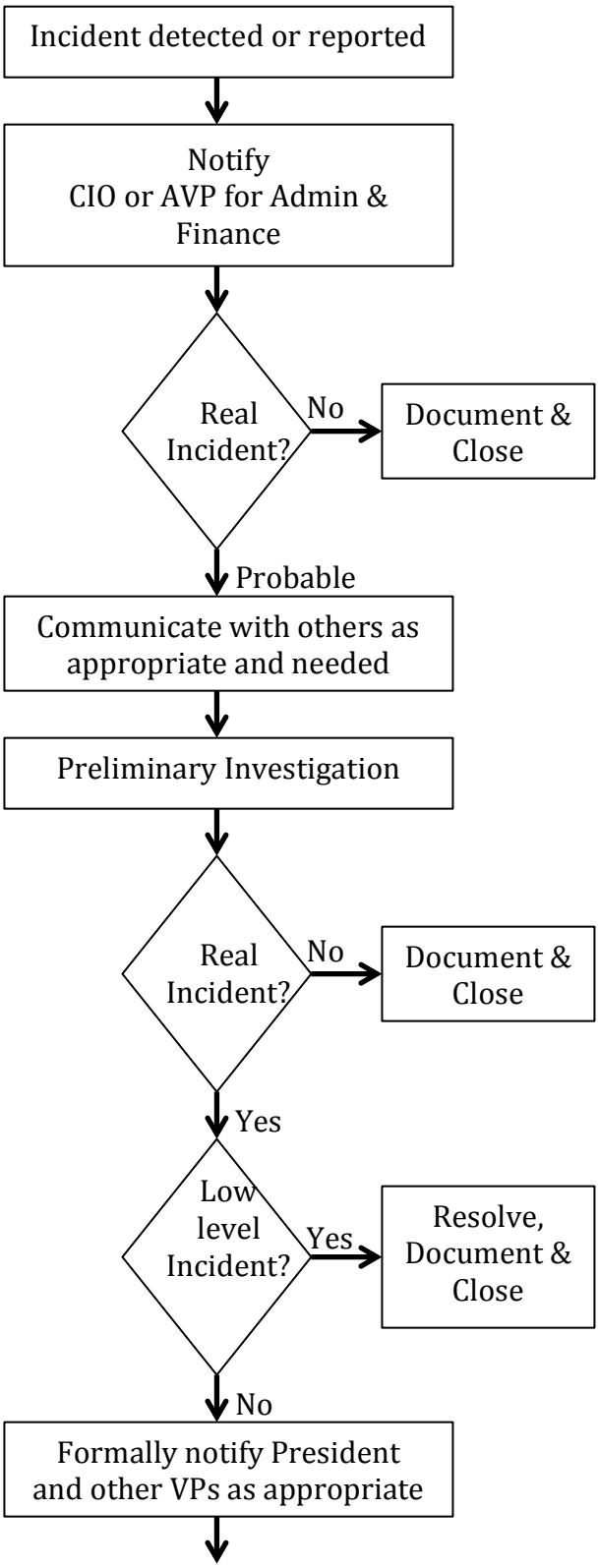
Security Incident Response Process



Notes

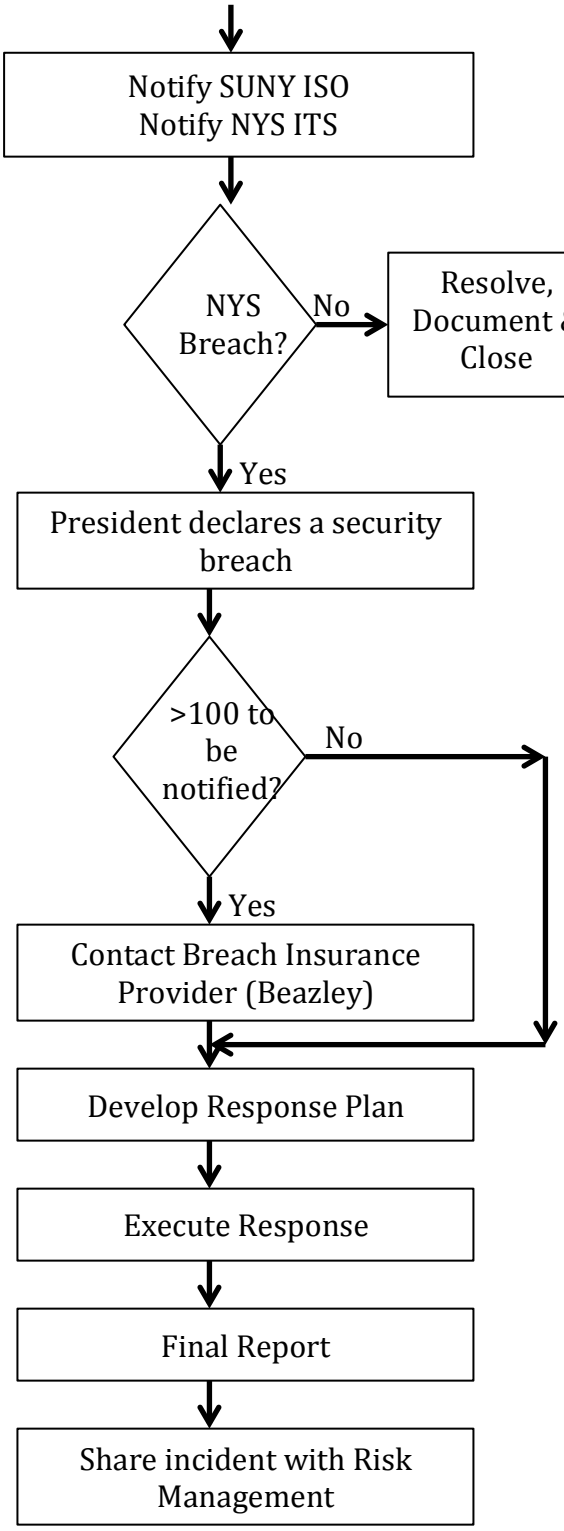
Detecting an incident can occur in many ways - Third party phone call/email, online form, internally detected, etc.

Preliminary fact gathering from reporter

CIT S&N, University Police, VPs, President, College Communications, Departments, ISEC team, SUNY Legal, Breach Insurance provider, SUNY SOC, NYS ITS

Was private information accessed by unauthorized person(s)?

Security Incident Response Process



Social Security Number, Bank Account Number, Credit Card Number, Motorist Id

- Notify Geneseo Board? CAS? ISEC Team? Others?
- Campus Announcement Needed?
- Preparation for Media Inquiries – Press Release?
- Identify and gather contact information for compromised individuals
- Determine if identity theft protection is needed based on level of risk
- Write external notification (SUNY Legal Template?/Beazley handling?)
- Do we need to adjust IT resources for a possible spike in traffic to our web site?

Definitions

Incident – any adverse event that threatens the confidentiality, integrity, or availability of college information assets, information systems, and the networks that deliver the information. Any violation of computer security policies, acceptable use polices, or standard computer security practices is an incident.

Adverse events may include unauthorized access, denial-of-service attacks, virus or malicious software, misuse of service, system or information, system intrusion, and reconnaissance scans and probes.

Low Level Incident – Incidents that have a minimal impact on the institutions business or services.

Low level incidents may be an isolated virus infection, nuisance malware, unauthorized access to data not protected by law and whose disclosure would cause no harm to the college or to individuals, username and password provided of an unpriviledged account through phishing

Security Breach – "Breach of the security of the system" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by a state entity.

An information security breach must be declared if there has been unauthorized access to any of the following private information.

1. Social Security Numbers
2. Motorist ID
3. Credit Card Numbers in combination with any required security code, access code, or password
4. Bank Account Numbers in combination with any required security code, access code, or password

CONTACTS

CIO

Susan E. Chichester
Chief Information Officer & Director, CIT
SUNY Geneseo
South Hall 119, 1 College Circle
Geneseo, NY 14454
Email: sue@geneseo.edu
585-245-5577 (Office)
585-245-5579 (Fax)

Associate Vice President, Administration and Finance

Brice Weigman
Associate Vice President, Administration and Finance
SUNY Geneseo
Doty 325F, 1 College Circle
Geneseo, NY 14454
Email: weigman@geneseo.edu
585-245-5606 (Office)

University Police

Thomas Kilcullen
Chief of the University, Police Department
SUNY Geneseo
Schrader Hall 19, 1 College Circle
Geneseo, NY 14454
Email: kilcullen@geneseo.edu
585-245-5651 (Office)
585-245-5653 (Fax)

System Administration

Ken Runyon, CISSP CISM
Chief Information Security Officer
Office of Information and Technology
The State University of New York
State University Plaza - Albany, New York 12246
Tel: 518.320.1368 Fax: 518.320.1550 Cell: 518.703.4086

New York State ITS

Cyber Command Center Hotline: 518-242-5045
NYS Watch Center: 518-292-2200
Email sycom@its.ny.gov
EISO PGP public key: http:/its.ny.gov/eiso/incident-reporting

Beazley Group: Breach Insurance Provider

Notification under this Policy:

(a) Claims:

Beazley Group
Attn: Beth Diamond
1270 Avenue of the Americas, 12th Floor
New York, NY 10020
Toll-Free 24-Hour Hotline: (866)567-8570
Fax: (646) 378-4039
Email: bbr.claims@beazley.com
(Calls to the above 24-hour hotline are immediately forwarded to the BBR response team)

(b) Privacy Breaches under Insuring Agreement I.B.:

Beazley Group
Attn: Beth Diamond
1270 Avenue of the Americas, 12th Floor
New York, NY 10020
Toll-Free 24-Hour Hotline: (866) 567-8570
Fax: (646) 378-4039
Email: bbr.claims@beazley.com
(Calls to the above 24-hour hotline are immediately forwarded to the BBR response team)

(c) All other notices under this Policy shall be given to:
Beazley USA Services, Inc.
30 Batterson Park Road
Farmington, CT 06032
Tel: (860) 677-3700
Fax: (860) 679-0247
(All Claims and Privacy Breaches should be reported in accordance with 9.(a) and 9.(b) of the policy)

NOTICE OF CLAIM, LOSS OR CIRCUMSTANCE THAT MIGHT LEAD TO A CLAIM

A. *If any **Claim** is made against the **Insured**, the **Insured** shall forward, as soon as practicable upon knowledge of any of the **Insured Organization's** President; members of the Board of Directors; executive officers, including the Chief Executive Officer, Chief Operating Officer, and Chief Financial Officer; General Counsel, staff attorneys employed by the **Insured Organization**; Chief Information Officer; Chief Security Officer; Chief Privacy Officer; **Manager**; and*

*any individual in a substantially similar position as those referenced above, or with substantially similar responsibilities as those referenced above, irrespective of the exact title of such individual and any individual who previously held any of the above referenced positions, to the Underwriters through persons named in Item 9.(a) of the Declarations written notice of such **Claim** in the form of a telecopy, email or express or certified mail together with every demand, notice, summons or other process received by the **Insured** or the **Insured's** representative. Notwithstanding the foregoing, in no event shall the Underwriters be given notice of a **Claim** later than the end of the **Policy Period**, the end of the **Optional Extension Period** (if applicable), or sixty (60) days after the expiration date of the **Policy Period** in the case of **Claims** first made against the **Insured** during the last sixty (60) days of the **Policy Period**.*

B.

*B. With respect to Insuring Agreement B., for a legal obligation to comply with a **Breach Notice Law** because of an incident (or reasonably suspected incident) described in Insuring Agreement A.1. or A.2., such incident or reasonably suspected incident must be reported as soon as practicable during the **Policy Period** after discovery by the **Insured** via the email address or telephone number set forth in Item 9.(b) of the Declarations; provided, that unless the **Insured** cancels the Policy, or the Underwriters cancel for non-payment of premium, incidents discovered by the **Insured** within sixty (60) days prior to expiration of the Policy shall be reported as soon as practicable, but in no event later than sixty (60) days after the end the **Policy Period**; provided further, that if this Policy is renewed by the Underwriters and **Privacy Breach Response Services** are provided because of such incident or suspected incident that was discovered by the Insured within sixty (60) days prior to the expiration of the Policy, and first reported during the sixty (60) day post **Policy Period** reporting period, then any subsequent **Claim** arising out of such incident or suspected incident is deemed to have been made during the **Policy Period**. Notwithstanding the foregoing, if the **Named Insured** reasonably believes that the **Privacy Breach Response Services** provided as a result of such incident or suspected incident are not likely to meet or exceed the **Retention**, then reporting of such incident or suspected incident under this Clause X.B. is at the **Named Insured's** option, but unless such incident or suspected incident is reported in accordance with the first paragraph of this Clause X.B., there shall be no coverage for **Privacy Breach Response Services** in connection with such incident or suspected incident.*

*C. If during the **Policy Period**, the **Insured** becomes aware of any circumstance that could reasonably be the basis for a **Claim** it may give written notice to the Underwriters in the form of a telecopy, email or express or certified mail through persons named in Item 9.(a) of the Declarations as soon as practicable during the **Policy Period**. Such a notice must include: 1. the specific details of the act, error, omission, or **Security Breach** that could reasonably be the basis for a **Claim**; 2. the injury or damage which may result or has resulted from the circumstance; and 3. the facts by which the **Insured** first became aware of the act, error, omission*

*or **Security Breach**. Any subsequent **Claim** made against the **Insured** arising out of such circumstance which is the subject of the written notice will be deemed to have been made at the time written notice complying with the above requirements was first given to the Underwriters. An incident or reasonably suspected incident reported to Underwriters during the **Policy Period** and in conformance with Clause X.B. shall also constitute notice of a circumstance under this Clause X.C.*

D. *A Claim or legal obligation under paragraph A. or B. above shall be considered to be reported to the Underwriters when written notice is first received by the Underwriters in the form of a telecopy, email or express or certified mail or email through persons named in Item 9.(a) of the Declarations of the Claim or legal obligation, or of an act, error, or omission, which could reasonably be expected to give rise to a Claim if provided in compliance with paragraph C. above.*