GENERAL DATA PROTECTION REGULATION (GDPR) PROCEDURES

INTRODUCTION 1
DEFINITIONS 1
Consent of the Data Subject 1
Controller 1
Data Event 1
Data Subject 1
DPO 1
Filing System 1
GDPR 1
High Risk 1
Information and Communications System 1
Personal Data 1
Personal Data Breach 1
Processor 2
Processing, Process, Processed, or Processes 2
Special Category of Personal Data 2
ENFORCEMENT PROCEDURES 2
Monitoring Procedure 2
TRAINING PROCEDURES 2
GENERAL PRIVACY PROCEDURES 2
Lawfulness of Processing 2
Determining Whether Processing Exceeds the Initial Purpose for Processing Personal Data Procedure 2
Consent Procedure 2
Consent from Children 3
CONTROLLER PROCEDURES 3
Notice and Transparency Procedure 3
Data Protection by Design and Default 4
Data Protection Impact Assessments 4
Incident Response Procedure 5
Data Processing Contracts Procedure 5
Record of Processing Activities Procedure 6
Notifications about Automated Processing Procedure 6

Security of Processing Procedure 6
Notification of a Data Breach to Supervisory Authorities Procedure 6
Communication of a Personal Data Breach to the Data Subject Procedure 7
Data Protection Officer Procedure 7
Autonomy of Data Protection Officer Procedure 8
Data Protection Officer Tasks Procedure 8
International Data Transfers via Appropriate Safeguards Procedure 9
PROCESSOR PROCEDURES 9
Data Processing Contracts Procedure 9
Security of Processing Procedure 10
Record of Processing Activities 10
Notification of a Personal Data Breach to a Controller 10
DATA SUBJECTS' RIGHTS 11
Right of Access Requirement Procedure 11
Rectification Procedure 12
Erasure or Blocking Requirement Procedure 13
Right to Restrict Processing Procedure 13
Data Portability Procedure 14
Right to Object Procedure 15
Automated Individual Decision-Making, Including Profiling Procedure 15

Introduction

The General Data Protection Regulation (GDPR) is a regulation under European Union (EU) law relating to data protection and privacy for all individuals within the EU.

It was adopted on 14 April 2016 and will come into effect on 25 May 2018, replacing the 1995 Data Protection Directive. The GDPR standardizes data protection laws across the EU member states, and requires businesses to take measures to protect the personal information and privacy of individuals.

The GDPR also regulates the transfer of personal information outside the EU. The Genmarc Group conducts business which includes services that involve handling personal information and is therefore affected by the GDPR.

This document sets out measures that Genmarc Research is taking to protect personal information and ensure compliance with the GDPR

DEFINITIONS

Consent of the Data Subject: Any freely given, specific, informed, and unambiguous indication of will, whereby the Data Subject agrees to the Processing of Personal Data about and/or relating to him or her. Consent shall be evidenced by written, electronic, or recorded means. It may also be given on behalf of the Data Subject by an agent specifically authorized by the Data Subject to do so.

Controller: A person or organization who alone or jointly with others determines the purposes and means of Processing of Personal Data.

Data Event: An occurrence within a Filing System.

Data Subject: An individual who's Personal Data is Processed.

DPO: Data Privacy Officer.

Filing System: Any structured set of personal data which are accessible according to specific criteria, in such a way that specific information relating to a particular person is readily accessible.

GDPR: EU Regulation 2016/679.

High Risk: Whenever this document uses the term "high risk" it means an activity that has a high probability of:

1. Risking the rights and freedoms of natural persons;
2. Causing physical, material, or non-material damage to a natural person;
3. Causing discrimination, identity theft, fraud, financial loss, damage to reputation, loss of confidentiality of Personal Data, unauthorized reversal of pseudonymization, or other significant economic or social harm;
4. Processing Personal Data regarding racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, genetic data, health, sex life, criminal convictions or offences;
5. Processing an employee's performance or reliability; Processing personal attributes about an individual such as economic situation, personal preferences or interests, reliability or behavior, location or movements to create or use personal profiles;
6. Processing information belonging to vulnerable sets of people such as children; or
7. Processing large volumes of Personal Data that affects a large number of data subjects.

Information and Communications System: A system for generating, sending, receiving, storing or otherwise Processing electronic data messages or electronic documents and includes the computer system or other similar device by or which data is recorded, transmitted, or stored and any procedure related to the recording, transmission, or storage of electronic data, electronic message, or electronic document.

Personal Data: Any information relating to an identified or identifiable data subject who can be identified, directly or indirectly, from that information.

Personal Data Breach: A breach of security leading to an accident or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

Processor: Any person (other than the staff of the Controller) or organization that Processes Personal Data on behalf of a Controller. A group company that Processes Personal Data for the Controller will be a Processor.

Processing, Process, Processed, or Processes: Any operation or any set of operations performed upon Personal Data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction of data.

Special Category of Personal Data: Refers to Personal Data:

1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical, or political affiliations; or
2. About an individual's health, education, genetic, or sexual life, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings.

ENFORCEMENT PROCEDURES

Monitoring Procedure: Genmarc Research ensures that all requirements contained in the GDPR Procedures are properly implemented by annually reviewing the documents listed in Exhibit 1 and determining whether the entries in those documents comply with the GDPR Policy.

TRAINING PROCEDURES

Every year, Genmarc Research will provide a copy of the GDPR Procedures to its officers and employees and have such individuals review that document. After review, those individuals must sign the GDPR Training Acknowledgement Form.

Genmarc Research will provide a copy of the GDPR Procedures to every new employee and have each new employee sign the GDPR Training Acknowledgement Form, attached as Exhibit 2, within a month of their hire date.

Puneet Puri will review the GDPR Tracking Sheet, attached as Exhibit 3, every quarter and make sure all officers and employees have signed the GDPR Training Acknowledgement Form.

GENERAL PRIVACY PROCEDURES

Lawfulness of Processing: When Genmarc Research wishes to rely upon legitimate interests as the basis of Processing, Puneet Puri will fill out the form attached as Exhibit 4. Genmarc Research will only rely upon legitimate interests where it is satisfied that those legitimate interests are not overridden by the rights and interests of the Data Subjects concerned.

Determining Whether Processing Exceeds the Initial Purpose for Processing Personal Data Procedure: Whenever Genmarc Research needs to determine if additional processing exceeds the initial purpose for Processing Personal Data, or a category of Personal Data, Genmarc Research will fill out and follow the instructions in Exhibit 5.

Consent Procedure: Whenever Genmarc Research uses consent as a legal basis for Processing, Genmarc Research will follow these steps:

1. Provide Data Subjects a Notice, in accordance with the Notice and Transparency Procedure below, and a request for Consent ("Consent Request") in a clearly distinguishable manner that is in an intelligible and easily accessible form;
2. The Consent Request will use clear and plain language;
3. The Consent Request will have Data Subjects actively opt-into the Consent Request. Pre-ticked boxes, opt-out boxes or default settings should be avoided;
4. Genmarc Research will, at the time of the Consent Request inform Data Subjects they have the right to withdraw consent, and provide Puneet Puri's contact information to withdraw consent; and
5. Genmarc Research will demonstrate that the Data Subject has consented to Processing of Personal Data by keeping records of such consent.

Consent from Children: Whenever Genmarc Research uses consent as the legal basis for Processing and intends to Process Personal Data from a Data Subject who is between the ages of 13 and 16, Genmarc Research will follow the Consent Procedure and the following additional steps:

1. Authenticate the identity of the person who has parental authority over the child;
2. Gather consent from a person with parental authority over the child by:
    a. Having such person sign a consent form and send it to Puneet Puri via fax, mail, or electronic scan; or
    b. Having such person call a toll-free number staffed by trained personnel;
3. If applicable, have the person with parental authority over the child use a credit card, debit card, or other online payment system that provide notification of each separate transaction to the account holder; and
4. Inform the person with parental authority over the child that they have the right to withdraw consent.

Genmarc Research will not use consent as a legal basis for Processing Personal Data belonging to children younger than 13 years of age.

CONTROLLER PROCEDURES

Notice and Transparency Procedure: Whenever Genmarc Research Processes Personal Data, it will provide Data Subjects with a notice. Genmarc Research will provide this notice at the time they obtain the Personal Data from the Data Subject. Such notice will include:

1. Genmarc Research's identify and contact details and where applicable, its representative;
2. The contact details for Genmarc Research's data protection officer, where applicable;
3. The purpose and legal basis for Processing the Personal Data;
4. Where applicable, the legitimate interests pursued by Genmarc Research or a third party;
5. Where the Personal Data was obtained from a source other than the Data Subject, the categories of Personal Data;
6. A list of recipients or categories of recipients who receive Personal Data, if any;
7. Where applicable, Genmarc Research's intent to transfer Personal Data to a third country or international organization and the following:
    a. The existence of an adequacy decision by the European Commission, or
    b. References to appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;
8. The period for which the personal data will be stored, or if that is not possible the criteria used to determine that period;

9. The existence of the right to request access to and rectify or erase Personal Data, or restrict Genmarc Research's Processing of Personal Data;
10. Where Processing is based on consent, the existence of the right to withdraw consent at any time;
11. The right to lodge a complaint with a supervisory authority;
12. Whether the provision of Personal Data is statutory or a contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and of the possible consequence of failure to provide such data;
13. The existence of automated decision-making, including profiling, where decisions are made solely on automated processing and where the decision has a legal effect or similarly significant effect. If either such methods are used to Process Personal Data, Genmarc Research will provide the Data Subject with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject; and
14. If Genmarc Research intends to Process Personal Data for purposes that extend beyond the initial purpose for Processing, Genmarc Research will provide the information above before additional Processing takes place.

These requirements do not apply if the Data Subject already has the information. Where the Data Subject is a child, the notice should be written in clear and plain language that a child will understand.

Genmarc Research will provide the information above by filling out Exhibit 6 and posting the completed exhibit to a publicly available website.

If Genmarc Research obtains Personal Data from a source other than the Data Subject, Genmarc Research will provide the Data Subject a link to the above-mentioned website no later than one month after obtaining the Personal Data.

Data Protection by Design and Default: Genmarc Research will, at the time of determining how it will Process Personal Data and at the time of Processing such data, implement appropriate technical and organizational measures designed to implement data-protection principles. Genmarc Research will implement appropriate technical and organizational measures to ensure that, by default, only the Personal Data that is necessary for each specific purpose is Processed.

Data Protection Impact Assessments: Genmarc Research will carry out a Data Protection Impact Assessment prior to any new Processing.

The Data Protection Impact Assessment will ensure Genmarc Research:

1. Implements appropriate technical and organizational measures for ensuring, by default, it only Processes Personal Data necessary for a specific purpose. This requirement applies to the amount of Personal Data collected, the extent of Processing, retention periods, and to the Personal Data;
2. Ensures, by default, Personal Data is not accessible without an individual's intervention with a natural person;
3. Describes the envisaged Processing operations and the purposes of the Processing, including, where applicable, the legitimate interest pursued by Genmarc Research;
4. Assesses the necessity and proportionality of the Processing operations in relates to its purpose;

5. Assesses the risks to the rights and freedoms of Data Subjects; and
6. Measures the envisaged Processing to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with the GDPR.

Wherever a Data Protection Impact Assessment reveals that proposed Processing may create a high risk to the rights of Data Subjects in the European Economic Area, Genmarc Research will revise the proposed Processing until it no longer creates a high risk to such individuals.

Where a type of Processing that uses new technologies may result in a high risk to the rights and freedoms of natural persons residing in the European Economic Area, Genmarc Research will, before Processing, conduct a Data Protection Impact Assessment to assess the impact of the Processing. Genmarc Research will seek out the advice of its data protection officer (DPO), if applicable, when carrying out the Data Protection Impact Assessment.

While Genmarc Research should carry out a Data Protection Impact Assessment prior to any new Processing as outlined above, the Data Protection Impact Assessment is required when:

1. Genmarc Research systematically and extensively evaluates personal aspects relating to natural persons with an automated Process, including profiling, wherein decisions with legal effects are produced;
2. Processing on a large scale of Special Personal Data or criminal convictions or offenses; or
3. Systematic monitoring of a publicly accessible area on a large scale.

Incident Response Procedure: Puneet Puri will follow the Incident Response Framework and use the Incident Report attached in Exhibit 8 whenever a Data Event could compromise the security of Personal Data.

Data Processing Contracts Procedure: Genmarc Research may engage Processors to Process Personal Data on its behalf if:

1. The Processor provides sufficient guarantees to implement appropriate technical and organizational measures to protect the rights of Data Subjects and comply with the GDPR.
2. The Processor agrees not to engage another Processor without prior specific or general written authorization from Genmarc Research. In such instances, the Processor must tell about any changes and give Genmarc Research an opportunity to object to such changes.
3. Genmarc Research and Processor enter into a contract setting out:
    a. What categories of Personal Data will be Processed;
    b. The duration of Processing;
    c. The nature and purpose of Processing;
    d. The type of Personal Data;
    e. The categories of Data Subjects involved; and
    f. Genmarc Research's rights.

    Such contract must also stipulate that the Processor:

    a. Only Processes Personal Data with Genmarc Research's instructions, including with regard to transfers of Personal Data to a third country or an international organization;

b. Ensures that persons who will Process Personal Data on the Processor's behalf have committed themselves to confidentiality or are under a statutory obligation of confidentiality;
c. Implement security measures consistent with the GDPR;
d. Will apply all the requirements in this section, **Data Processing Contracts Procedure**, to other Processors;
e. Assists Genmarc Research when a Data Subject makes a request to exercise their rights;
f. At Genmarc Research's choice, deletes or returns all Personal Data to Genmarc Research when the Processor no longer provides services to Genmarc Research; and
g. Will make available information necessary to demonstrate compliance with the requirements in this section, **Data Processing Contracts Procedure**, and contributes to audits or inspections from Genmarc Research or Genmarc Research's designee. Processor may inform Genmarc Research if, in its opinion, an instruction infringes the GDPR or other law from the European Union or one of its member states' laws.

Exhibit 9 can be used as a contract template containing the requirements above.

Record of Processing Activities Procedure: For each of Genmarc Research's subsidiaries or affiliates, that are Controllers or joint Controllers, Puneet Puri will fill out the document attached as Exhibit 10.

Notifications about Automated Processing Procedure: Whenever Genmarc Research automatically Processes information and that Processing is the sole basis for making a decision about a Data Subject, and when the decision would produce legal effects or otherwise significantly affect the Data Subject, Genmarc Research will direct Data Subjects to its Notice which is attached as Exhibit 6.

Security of Processing Procedure: Genmarc Research adopts the procedures and controls in Exhibits 21 and 22, based on the Center For Internet Security's 20 Critical Controls, as the framework for its security program.

Notification of a Data Breach to Supervisory Authorities Procedure: As part of Genmarc Research's recurring training, Puneet Puri will inform all Genmarc Research employees of their respective roles in this Notification of a Data Breach to Supervisory Authorities Procedure.

In the event of a suspected Personal Data Breach, any Genmarc Research employee will immediately report the suspected Personal Data Breach to their immediate supervisor.

If the employee does not have an immediate supervisor, or that supervisor is unavailable or does not respond within 8 hours, the employee will report the suspected breach to Puneet Puri.

All supervisors must immediately reported any suspected Personal Data Breaches to Puneet Puri.

Puneet Puri will immediately conduct a preliminary investigation to determine if a Personal Data Breach occurred and if the Personal Data Breach is likely to result in a high risk to natural persons residing in the European Economic Area.

If Puneet Puri determines that the Personal Data Breach is likely to result in a high risk to natural persons residing in the European Economic Area, Genmarc Research will—within 72 hours after having become aware of it—provide appropriate supervisory authorities a filled out copy of Exhibit 8, Event Report.

If a notification to the supervisory authority is not made within 72 hours, Genmarc Research will explain the reason(s) for delay.

If Puneet Puri determines that the Personal Data Breach is unlikely to result in a high risk, Genmarc Research does not have to notify the appropriate supervisory authorities under this procedure.

Genmarc Research may provide information to supervisory authorities in phases without undue delay.

Genmarc Research will document any Personal Data Breaches, list the facts related to it, its effects, and remedial action taken.

Communication of a Personal Data Breach to the Data Subject Procedure: When a Personal Data Breach is likely to result in a high risk to a natural person residing in the European Economic Area, Genmarc Research will communicate the Personal Data Breach to the Data Subject without undue delay. Puneet Puri may use Exhibit 11 to satisfy this notification requirement.

As part of Genmarc Research's recurring training, Puneet Puri will inform all Genmarc Research employees of their respective roles in this Communication of a Personal Data Breach to the Data Subject Procedure.

In the event of a suspected Personal Data Breach, any Genmarc Research employee will immediately report the suspected Personal Data Breach to their immediate supervisor.

If the employee does not have an immediate supervisor, or that supervisor is unavailable or does not respond within 8 hours, the employee will report the suspected breach to Puneet Puri.

All supervisors must immediately report any suspected Personal Data Breaches to Puneet Puri.

Puneet Puri will immediately conduct a preliminary investigation to determine if a Personal Data Breach occurred and if Personal Data Breach is likely to result in a high risk to the rights and freedoms of a natural person residing in the European Economic Area.

Genmarc Research is not required to make the communication discussed above if any of the following conditions are met:

1. Genmarc Research has implemented appropriate technical and organizational protection measures, and those measures were applied to the Personal Data affected by the Personal Data Breach, in particular those that render the Personal Data unintelligible to any person not authorized to access the Personal Data, such as encryption;
2. Genmarc Research has taken subsequent measures which ensure that the high risk to the rights and freedoms of Data Subjects is no longer likely to materialize; or
3. It would involve disproportionate effort. In such case, there shall instead be a public communication or similar measure whereby Data Subjects are informed in an equally effective manner.

Genmarc Research will document any Personal Data Breaches, list the facts related to it, its effects, and remedial action taken.

Data Protection Officer Procedure: Genmarc Research will designate a Data Protection Officer (DPO) based on the individual's expert knowledge of data protection laws and practices and their ability to fulfill the tasks in the following section.

Puneet Puri may designate a staff member as the DPO, or may fulfill the tasks assigned to the DPO via service contract.

If a staff member, the DPO may fulfill other tasks and duties, so long as Genmarc Research ensures that these tasks and duties do not result in a conflict of interest. Positions such as CEO or senior roles
in IT, Marketing, Finance, or Human Resources will likely lead to conflicts.

Puneet Puri will disseminate a communication to all processors or controllers that may have access to Personal Data held by Genmarc Research, informing them of the identity and contact information of the DPO and that the DPO is Genmarc Research's point of contact for all Data Subject issues related to the Processing of Personal Data or the exercise of rights under the GDPR.

If Genmarc Research maintains a website, Puneet Puri will list the name and contact information of the DPO on that website. Puneet Puri will also publish to the website the fact that the DPO is Genmarc Research's point of contact for all Data Subject issues related to the Processing of Personal Data or the exercise of rights under the GDPR.

Puneet Puri will include the name and contact number of the DPO in notices given to Data Subjects pursuant to the GDPR. This notice will also inform data subjects that the DPO is Genmarc Research's point of contact for all Data Subject issues related to the Processing of Personal Data or the exercise of rights under the GDPR.

Puneet Puri will communicate the identity of the DPO and their contact details to the supervisory authority. Puneet Puri will inform the supervisory authority that the DPO is Genmarc Research's point of contact for all Data Subject issues related to the Processing of Personal Data or the exercise of rights under the GDPR.

Puneet Puri will disseminate a communication to Genmarc Research employees, informing them of the identity of the DPO and of the role of the DPO. This communication should also inform employees that the DPO is Genmarc Research's point of contact for all Data Subject issues related to the Processing of Personal Data or the exercise of rights under the GDPR.

Autonomy of Data Protection Officer Procedure: The DPO reports directly to the highest management level of Genmarc Research.

The DPO will disseminate a communication to Genmarc Research's employees, informing them that the DPO should not receive any instruction in exercising the tasks described in the Data Protection Officer Tasks Procedure.

The DPO will not be dismissed or penalized by Genmarc Research for performing the tasks described in the Data Protection Officer Tasks Procedure.

Data Protection Officer Tasks Procedure: The DPO will disseminate a communication to Genmarc Research's employees, informing them that the DPO is to be notified immediately of any issues related to the protection of Personal Data. Genmarc Research's employees will inform the DPO of any issues related to the protection of Personal Data as soon as they discover those issues.

Annually, the DPO will provide training to Genmarc Research's employees, advising them of their Processing obligations under the GDPR.

Annually, the DPO will review all of Genmarc Research's privacy policies and notices to Data Subjects to ensure compliance with the GDPR and member states' data protection provisions.

Annually, the DPO will audit Genmarc Research's compliance with its GDPR procedures and document those audits in Exhibit 1. The DPO should conduct both regularly scheduled audits and "no-notice" audits

under this procedure. For any finding of non-compliance in the above audits, the DPO will recommend corrective actions to the management of Genmarc Research and assist in their implementation as necessary.

Whenever Genmarc Research is required to conduct a Data Protection Impact Assessment, the DPO will review that assessment and make any necessary recommendations.

The DPO will review vendor contracts to ensure they provide the same level of protection for Personal Data as Genmarc Research.

The DPO will consult with the supervisory authority on all issues related to Processing, or as required by any other matter.

Genmarc Research's employees must refer any inquiries from supervisory authorities to the DPO.

International Data Transfers via Appropriate Safeguards Procedure: Puneet Puri will, to the maximum extent possible, incorporate standard data protection clauses adopted by the European Commission or the supervisory authority in all Genmarc Research contracts involving the transfer of Personal Data to a third country (outside the European Economic Area and where a finding of adequacy has not been made by the European Commission) or international organization.

If unable to incorporate the above standard data protection clauses, Puneet Puri will use a code of conduct certified by a supervisory authority and drafted by an association or other body representing controllers or processors.

If unable to use the above two procedures, Puneet Puri will ensure that all contracts involving the transfer of Personal Data to a third country or international organization includes provisions requiring the protection of Personal Data to the same extent that Genmarc Research would protect the Personal Data. Puneet Puri should use terms as similar as possible to the relevant standard data protection clauses adopted by the European Commission.

Puneet Puri will submit the contractual clauses from the above procedure to the supervisory authority for approval. Once those contractual clauses have been approved, Puneet Puri should use the approved clauses in subsequent contracts, as appropriate.

PROCESSOR PROCEDURES

Whenever Genmarc Research acts as a Processor, the following procedures will apply:

Data Processing Contracts Procedure: Genmarc Research may engage Processors to Process Personal Data on its behalf if:

1. The Processor provides sufficient guarantees to implement appropriate technical and organizational measures to protect the rights of Data Subjects and comply with the GDPR.
2. The Processor agrees not to engage another Processor without prior specific or general written authorization from Genmarc Research. In such instances, the Processor must tell Genmarc Research about any changes and give Genmarc Research an opportunity to object to such changes.
3. Genmarc Research and Processor enter into a contract setting out:
    a. What categories of Personal Data will be Processed;
    b. The duration of Processing;
    c. The nature and purpose of Processing;

d. The type of Personal Data;
e. The categories of Data Subjects involved; and
f. Genmarc Research's rights.

Such contract must also stipulate that the Processor:

a. Only Processes Personal Data with Genmarc Research's instructions, including with regard to transfers of Personal Data to a third country or an international organization;
b. Ensures that persons who will Process Personal Data on the Processor's behalf have committed themselves to confidentiality or are under a statutory obligation of confidentiality;
c. Implement security measures consistent with the GDPR;
d. Will apply all the requirements in this section, **Data Processing Contract Procedure**, to other Processors;
e. Assists Genmarc Research when a Data Subject makes a request to exercise their rights;
f. At Genmarc Research's choice, deletes or returns all Personal Data to Genmarc Research when the Processor no longer provides services to Genmarc Research; and
g. Will make available information necessary to demonstrate compliance with the requirements in this section, **Data Processing Contracts**, and contribute to audits or inspections from Genmarc Research or Genmarc Research's designee. Processor may inform Genmarc Research if, in its opinion, an instruction infringes the GDPR or other law from the European Union or one of its member states' laws.

Exhibit 9 can be used as a contract template containing the requirements above.

Security of Processing Procedure: Genmarc Research satisfies the conditions from the GDPR Policy for Security of Processing by filling out Exhibit 10. Genmarc Research adopts the Center For Internet Security's 20 Critical Controls as the framework for its security program.

Record of Processing Activities: Genmarc Research and, where applicable, its representative in the European Economic Area, will maintain records describing its Processing activities. Records will include:

1. Genmarc Research's name, the Genmarc Research's representative, and Genmarc Research's data protection officer;
2. The name, representative and data protection officer of each Controller on behalf of which Genmarc Research is Processing Personal Data.
3. Categories of Personal Data being Processed on behalf of each Controller;
4. Whether the Personal Data transfers to a third country or an entity outside the European Economic Area) that will be involved in the Processing and if so the country in question and the safeguards in place; and
5. A general description of the organizational, physical, or technical security measures in place.

Notification of a Personal Data Breach to a Controller: In the event of a Personal Data Breach, Puneet Puri will—within 72 hours after having become aware of it—provide appropriate Controllers a filled out copy of Exhibit 12, Event Report.

If a notification to the Controller is not made within 72 hours, Genmarc Research will explain the

reason(s) for delay.

Genmarc Research may provide information to Controllers in phases without undue delay.

DATA SUBJECTS' RIGHTS

Puneet Puri will be Genmarc Research's point of contact for all the procedures in this section. Puneet Puri will communication to Genmarc Research's employees that all Data Subject requests should be forwarded to Puneet Puri.

After verifying a Data Subject's identity, Genmarc Research will take appropriate measures to provide any information referred to in this section using concise, transparent, intelligible, and easily accessible form, using clear and plain language.

Genmarc Research will provide information when a Data Subject requests to exercise their rights listed in this section without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. Genmarc Research will inform the Data Subject of any such extension within one month of receipt of the request.

If Genmarc Research does not take action on the request of the Data Subject, Genmarc Research will inform the Data Subject without delay and at the latest within one month of receiving the Data Subject's request of the reasons for not taking action and inform the Data Subject that they may lodge a complaint with a supervisory authority.

Genmarc Research will not charge Data Subjects for receiving information for exercising their rights in this section.

When a Data Subject makes manifestly unfounded or excessive requests, Genmarc Research may charge a reasonable fee; or refuse to act on the request.

Puneet Puri will maintain a record of data requests, attached as Exhibit 13, reflecting the date of the request, date of response, and any reasons for delay.

Right of Access Requirement Procedure: Upon receipt of request, Puneet Puri will verify whether Genmarc Research is processing the requesting Data Subject's Personal Data.

If Genmarc Research is processing the requesting Data Subject's Personal Data, then Puneet Puri will respond by providing the data subject a copy of the Personal Data that Genmarc Research is processing and the following information:

1. The purpose of the Processing;
2. Contents of Processed Personal Data and the categories of Personal Data concerned;
3. The recipients or categories of recipients to whom the Personal Data have been or will be disclosed, in particular recipients in third countries or international organizations;
4. Where possible, the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period;
5. The existence of the right to request from the controller rectification or erasure of Personal Data or restriction of Processing of Personal Data concerning the Data Subject or to object to such Processing;
6. The right to lodge a complaint with the supervisory authority;

7. Where the Personal Data is not collected from the Data Subject, any available information as to its source;
8. The existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject;
9. Where Personal data is transferred to a third country or to an international organization, Genmarc Research will inform the Data Subject of the safeguards used to protect the transferred Personal Data;
10. Date when the Data Subject's Personal Data was last accessed and modified; and
11. The designation, name, and address of the Controller.

Puneet Puri will provide the information described above to the Data Subject within 30 days of receipt of the request. If, because of the complexity of the request, Genmarc Research is unable to comply within 30 days, Puneet Puri will inform the Data Subject of the need for an extension within 30 days of receipt of the request. The extension may be for up to two months.

If the Data Subject makes the request by electronic form, Puneet Puri will provide the above information by electronic means if possible, unless otherwise requested by the Data Subject.

When communicating the above information to the Data Subject, Puneet Puri will notify the Data Subject to contact Puneet Puri if they wish to rectify any inaccuracies or errors in the Personal Data they receive from Genmarc Research.

If Genmarc Research is not Processing the requesting Data Subject's Personal Data, they will notify the Data Subject that they are not processing the Personal Data.

Puneet Puri will document the actions taken pursuant to this procedure in Exhibit 14, Record of Data Subjects' Request for Access.

Rectification Procedure: Puneet Puri will provide Data Subjects access to their Personal Data pursuant to the Right of Access Procedure.

When Puneet Puri receives a rectification request from a Data Subject, including a request to complete what was previously incomplete Personal Data, Puneet Puri will verify the inaccuracy or incompleteness and coordinate with the appropriate persons within Genmarc Research to correct the Personal Data.

Puneet Puri will notify the Data Subject that their information has been corrected or completed and will provide the Data Subject with a copy of both the new and redacted Personal Data. Puneet Puri will also notify the Data Subject that the Data Subject may request the identity of third- party recipients who were told to rectify the Data Subject's data.

Puneet Puri will communicate any rectification of Personal Data to each third-party recipient to whom the Personal Data has been disclosed.

If Puneet Puri discovers the Data Subject's Personal Data is incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes, or is no longer necessary for the purposes for which it was initially collected, Puneet Puri will coordinate with the appropriate persons within Genmarc Research to suspend, withdraw, or order the blocking, removal, or destruction of the Data Subject's Personal Data from Genmarc Research's Filing System.

Puneet Puri will document the actions taken pursuant to this procedure in Exhibit 15, Record of Data Subjects' Request for Rectification.

Erasure or Blocking Requirement Procedure: When Puneet Puri receives a Data Subject's request for erasure, Puneet Puri will review Genmarc Research's Record of Processing Activities to determine the purpose and legal basis for Processing the Personal Data.

Based on the purpose and legal basis for Processing, Puneet Puri may review the following to determine if Genmarc Research is required to erase the Personal Data:

1. A Data Subject's Personal Data is no longer necessary for the purposes for which that Personal Data was collected;
2. A Data Subject withdraws consent (where Processing is on the basis of consent) or objects to Genmarc Research's Processing of the Data Subject's Personal Data and where there is no other legal ground for Processing;
3. The Data Subject objects to the Processing on the basis of automated decision making or direct marketing purposes and there are no overriding legitimate grounds for Processing;
4. Genmarc Research's Processing of a Data Subject's Personal Data is unlawful;
5. The Personal Data has to be erased for compliance with a legal obligation in the European Union or under the laws of one of its member states to which the controller is subject; and
6. The Personal Data has been collected in relation to the offer of information society services to an individual under the age of 16.

If one of the above applies, Puneet Puri will coordinate with the appropriate persons within Genmarc Research to erase the Personal Data from Genmarc Research's Filing System without undue delay.

If none of the above apply, Puneet Puri will notify the Data Subject that their Personal Data has not been erased and the reason(s) why.

Puneet Puri will notify relevant Controllers and third parties who work for or with Genmarc Research to delete the information pursuant to the Data Subject's request.

Puneet Puri will notify the Data Subject that their information has been erased. Puneet Puri will include in this notice that the Data Subject has the right to request the identity of third- party recipients Genmarc Research has notified about the erasure request.

Puneet Puri will document the actions taken pursuant to this procedure in Exhibit 16, Record of Data Subjects' Request for Erasure or Blocking.

Right to Restrict Processing Procedure: When Puneet Puri receives a Data Subject's request for restriction of Processing, Puneet Puri will review Genmarc Research's Record of Processing Activities to determine the purpose and legal basis for Processing the Personal Data.

Based on the purpose and legal basis for Processing, Puneet Puri will review the following to determine if the Data Subject has the right to restrict Processing:

1. The accuracy of the Personal Data is contested by the Data Subject, for a period enabling Genmarc Research to verify the accuracy of the Personal Data;

2. The Processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of its use instead;
3. The Controller no longer needs the Personal Data for the purposes of the Processing; and
4. The Data Subject has objected to Processing on the basis of automated decision making, and the determination of whether the legitimate grounds of the controller override those of the Data Subject is pending.

If a restriction on Processing is warranted under the first entry in the list above, Puneet Puri will coordinate with the appropriate persons within Genmarc Research to verify the accuracy of the Personal Data within 30 days.

If one of the entries in the list above applies, and the Personal Data is not being Processed for the exercise or defense of legal claims, for the protection of the rights of another, or for public interests reasons, Puneet Puri will notify the Data Subjects and obtain their consent in accordance with the CONSENT PROCEDURE prior to processing that Personal Data.

When Puneet Puri receives a Data Subject's request for restriction of Processing, Puneet Puri will review Genmarc Research's Record of Processing Activities to determine the purpose and legal basis for Processing the Personal Data.

Based on the purpose and legal basis for processing, Puneet Puri will review the following to determine if the data subject has the right to restrict processing:

1. The accuracy of the Personal Data is contested by the Data Subject, for a period enabling Genmarc Research to verify the accuracy of the Personal Data;
2. The Processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of its use instead;
3. The controller no longer needs the Personal Data for the purposes of the Processing; and
4. The Data Subject has objected to Processing on the basis of automated decision making, and the determination of whether the legitimate grounds of the controller override those of the Data Subject is pending.

If a restriction on Processing is warranted under number one in the above list, Puneet Puri will coordinate with the appropriate persons within Genmarc Research to verify the accuracy of the Personal Data within 30 days.

If one of the above applies, and the Personal Data is not being Processed for the exercise or defense of legal claims, for the protection of the rights of another, or for public interests reasons, Puneet Puri will notify the Data Subject's and obtain their consent in accordance with the CONSENT PROCEDURE prior to processing that Personal Data.

Puneet Puri will document the actions taken pursuant to this procedure in Exhibit 17, Record of Data Subject's Request for Restriction on Processing.

Data Portability Procedure: Puneet Puri will review the Record of Processing and determine what Processing activities are carried out via automated means. Wherever Genmarc Research uses automatic means to Process Personal Data, Puneet Puri will coordinate with relevant people in Genmarc Research to develop a standardized, commonly used, machine-readable format for providing such information.

Once Puneet Puri has developed this standardized format, Genmarc Research will use that format when providing information to Data Subjects.

Right to Object Procedure: Puneet Puri ensures Genmarc Research's privacy notices tell Data Subjects they may object to Genmarc Research's use of Personal Data if Genmarc Research's legal basis for processing is premised on the public interest or Genmarc Research's legitimate business interests. Such notice will tell Data Subjects they can exercise their right to object by notifying Puneet Puri

When Genmarc Research receives a request objecting to Genmarc Research's Processing, Puneet Puri will review Genmarc Research's purpose for Processing in the Record of Processing. Unless Genmarc Research has a compelling legitimate purpose that overrides the Data Subject's rights, Puneet Puri will recommend Genmarc Research and appropriate departments/people comply with the Data Subject's objection.

When a Data Subject objects to direct marketing, Puneet Puri will work with relevant departments and people from Genmarc Research to comply with the Data Subject's request.

Puneet Puri will document the actions taken pursuant to this procedure in Exhibit 18, Record of Data Subjects' Objections to Processing.

Automated Individual Decision-Making, Including Profiling Procedure: If Genmarc Research uses automated decision making, Genmarc Research will disclose the following to Data Subjects:

1. Notice that Genmarc Research engages in automated decision making and the categories of information that undergo automated decision making;
2. Meaningful information about the logic involved; and
3. An explanation of the significance and potential consequences associated with automated decision making.

If a Data Subject exercises their right not to be subject to a decisions based solely on automated decision making, Puneet Puri will review the automatic Processes and determine whether automated decision making:

1. Is necessary for entering into, or performance of, a contract between Genmarc Research and the Data Subject;
2. Is authorized by the European Union or the laws of one of its member states; or
3. Is based on the Data Subject's explicit consent.

If one of the above applies, Puneet Puri will notify the Data Subject about the exception and the decision to continue automated decision making to Process his or her Personal Data.

Puneet Puri will coordinate with appropriate persons within Genmarc Research to ensure such automated processing is not based on Special Personal Data unless (i) the processing is necessary for reasons of substantial public interest, as set out in the relevant member state law; or (ii) Genmarc Research has obtained explicit consent.

If Puneet Puri determines such automated Processing is permitted by member state law as being in the substantial public interest, Puneet Puri may authorize such automated processing, but will document that authorization in Exhibit 19, Record of Authorization to Automatically Process

Special Personal Data, and each quarter review Exhibit 19 and determine if automated processing is still required.

If a Data Subject explicitly consents to such automated Processing of Special Personal Data, Puneet Puri will record that consent in Exhibit 19, Record of Authorization to Automatically Process Special Personal Data.

Puneet Puri will coordinate with appropriate persons within Genmarc Research to conduct regular quality assurance checks of their systems to make sure that individuals are being treated fairly and not discriminated against, whether on the basis of Special Personal Data or otherwise.

Puneet Puri will coordinate with appropriate persons within Genmarc Research to test the algorithms used and developed by machine learning systems to prove they perform as intended, and not producing discriminatory, erroneous, or unjustified results.

Puneet Puri will coordinate with appropriate persons within Genmarc Research to use anonymisation or pseudonymisation techniques in the context of profiling.

Puneet Puri will coordinate with appropriate persons within Genmarc Research to provide a mechanism for human intervention in defined cases, for example providing a link to an appeals process at the point the automated decision is delivered to the Data Subject, with agreed timescales for the review and a named contact point for any queries.

Puneet Puri will document objection to automatic Processing in Exhibit 20, Record of Data Subjects' Objections to Automated Processing.

EFFECTIVE DATE

This document shall take effect on **05/24/2018**. All previous issuances of this document that are inconsistent with the whole or any part of these GDPR Procedures are revoked and superseded.

ADMINISTRATION

This document will be administered by Puneet Puri.

Puneet Puri shall retain the right to amend, revoke, withdraw, or nullify the whole or any part of this document.

Exhibit 1

Security of Processing: Security Procedures

Genmarc Research's security procedures are derived from the Center for Internet Security's 20 Critical Controls and are as follows:

Procedure 1: Inventory of Authorized and Unauthorized Devices: Genmarc Research actively manages (by inventorying, tracking, and correcting) all hardware devices on its networks so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Procedure 2: Inventory of Authorized and Unauthorized Software: Genmarc Research actively manages (by inventorying, tracking, and correcting) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Procedure 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers: Genmarc Research will establish, implement, and actively manage (by tracking, reporting on, and correcting) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers form exploiting vulnerable services and settings.

Procedure 4: Continuous Vulnerability Assessment and Remediation: Genmarc Research will continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

Procedure 5: Controlled Use of Administrative Privileges: Genmarc Research will uses tools and/or processes to track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

Procedure 6: Maintenance, Monitoring, and Analysis of Audit Logs: Genmarc Research will collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

Procedure 7: Email and Web Browser Protections: Genmarc Research will minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

Procedure 8: Malware Defenses: Genmarc Research will control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

Procedure 9: Limitation and Control of Network Ports, Protocols, and Services: Genmarc Research will Manage (by tracking/controlling/correcting) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

Control 10: Data Recovery Capability: Genmarc Research uses processes and tools to properly back up critical information with a proven methodology for timely recovery of such information.

Procedure 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches: Genmarc Research will establish, implement, and actively manage (by tracking, reporting on, correcting) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Procedure 12: Boundary Defense: Genmarc Research will detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

Procedure 13: Data Protection: Genmarc Research will implement processes and tools to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

Procedure 14: Controlled Access Based on the Need to Know: Genmarc Research uses processes and tools to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Procedure 15: Wireless Access Control: Genmarc Research uses processes and tools to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

Procedure 16: Account Monitoring and Control: Genmarc Research actively manages the life cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.

Procedure 17: Security Skills Assessment and Appropriate Training to Fill Gaps: For all functional roles within Genmarc Research (prioritizing those mission-critical to the business and its security), Genmarc Research will identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

Procedure 18: Application Software Security: Genmarc Research manages the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

Procedure 19: Incident Response Management: Genmarc Research protects its information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

Procedure 20: Penetration Tests and Red Team Exercises: Genmarc Research will test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

Exhibit 2

Security of Processing: Security Controls

Genmarc Research has adopted the controls below to implement its Security Procedures. These controls and their corresponding procedures come from the Center for Internet Security's 20 Critical Controls.

Procedure 1: Inventory of Authorized and Unauthorized Devices

Control 1.1: Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.

Control 1.2: If the organization is dynamically assigning addresses using DHCP, then deploy dynamic host configuration protocol (DHCP) server logging, and use this information to improve the asset inventory and help detect unknown systems.

Control 1.3: Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.

Control 1.4: Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.

Control 1.5: Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems.

Control 1.6: Use client certificates to validate and authenticate systems prior to connecting to the private network.

Procedure 2: Inventory of Authorized and Unauthorized Software

Control 2.1: Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.

Control 2.2: Deploy application whitelisting that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require

only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.

Control 2.3: Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. The software inventory systems must be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.

Control 2.4: Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations but based on higher risk should not be installed within a networked environment.

Procedure 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Control 3.1: Establish standard secure configurations of operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.

Control 3.2: Follow strict configuration management, building a secureimage that is used to build all new systems that are deployed in the enterprise. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates or exceptions to this image should be integrated into the organization's change management processes. Images should be created for workstations, servers, and other system types used by the organization.

Control 3.3: Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air- gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.

Control 3.4: Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

Control 3.5: Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The reporting system should: have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command). These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).

Control 3.6: Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur. This

Includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system. Whenever possible use tools compliant with the Security Content Automation Protocol (SCAP) in order to streamline reporting and integration.

Control 3.7: Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for UNIX systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals. They should be capable of triggering redeployment of configuration settings on a scheduled, manual, or event-driven basis.

Procedure 4: Continuous Vulnerability Assessment and Remediation

Control 4.1: Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).

Control 4.2: Correlate event logs with information from vulnerability scans to fulfill two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools is itself logged. Second, personnel should be able to correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable.

Control 4.3: Perform vulnerability scanning in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested. Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses. Ensure that only authorized employees have access to the vulnerability management user interface and that roles are applied to each user.

Control 4.4: Subscribe to vulnerability intelligence services in order to stay aware of emerging exposures, and use the information gained from this subscription to update the organization's vulnerability scanning activities on at least a monthly basis. Alternatively, ensure that the vulnerability scanning tools you use are regularly updated with all relevant important security vulnerabilities.

Control 4.5: Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.

Control 4.6: Monitor logs associated with any scanning activity and associated administrator accounts to ensure that this activity is limited to the timeframes of legitimate scans.

Control 4.7: Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed, either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk. Such acceptance of business risks for existing vulnerabilities

Should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed, increasing the risk.

Control 4.8: Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers, desktops, laptops). Apply patches for the riskiest vulnerabilities first. A phased rollout can be used to minimize the impact to the organization. Establish expected patching timelines based on the risk rating level.

Procedure 5: Controlled Use of Administrative Privileges

Control 5.1: Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Control 5.2: Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.

Control 5.3: Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.

Control 5.4: Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.

Control 5.5: Configure systems to issue a log entry and alert on any unsuccessful login to an administrative account.

Control 5.6: Use multi-factor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards, certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.

Control 5.7: Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

Control 5.8: Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems.

Control 5.9: Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading email, composing documents, or surfing the Internet.

Procedure 6: Maintenance, Monitoring, and Analysis of Audit Logs

Control 6.1: Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.

Control 6.2: Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

Control 6.3: Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

Control 6.4: Have security personnel and/or system administrators run biweekly reports that identify anomalies in logs. They should then actively review the anomalies, documenting their findings.

Control 6.5: Configure network boundary devices, including firewalls, network-based IPS, and inbound and outbound proxies, to verbosely log all traffic (both allowed and blocked) arriving at the device.

Control 6.6: Deploy a SIEM (Security Information and Event Management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using the SIEM tool, system administrators and security personnel should devise profiles of common events from given systemsso that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.

Procedure 7: Email and Web Browser Protections

Control 7.1: Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers provided by the vendor in order to take advantage of the latest security functions and fixes.

Control 7.2: Uninstall or disable any unnecessary or unauthorized browser or email client plugins or add-on applications. Each plugin shall utilize application / URL whitelisting and only allow the use of the application for pre-approved domains.

Control 7.3: Limit the use of unnecessary scripting languages in all web browsers and email clients. This includes the use of languages such as ActiveX and JavaScript on systems where it is unnecessary to support such capabilities.

Control 7.4: Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.

Control 7.5: Deploy two separate browser configurations to each system. One configuration should disable the use of all plugins, unnecessary scripting languages, and generally be configured with limited functionality and be used for general web browsing. The other configuration shall allow for

more browser functionality but should only be used to access specific websites that require the use of such functionality.

Control 7.6: The organization shall maintain and enforce network based URL filters that limit a system's ability to connect to websites not approved by the organization. The organization shall subscribe to URL categorization services to ensure that they are up-to- date with the most recent website category definitions available. Uncategorized sites shall be blocked by default. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.

Control 7.7: To lower the chance of spoofed email messages, implement the Sender Policy Framework (SPF) by deploying SPF records in DNS and enabling receiver-side verification in mail servers.

Control 7.8: Scan and block all email attachments entering the organization's email gateway if they contain malicious code or file types that are unnecessary for the organization's business. This scanning should be done before the email is placed in the user's inbox. This includes email content filtering and web content filtering.

Procedure 8: Malware Defenses

Control 8.1: Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.

Control 8.2: Employ anti-malware software that offers a centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying an update, automated systems should verify that each system has received its signature update.

Control 8.3: Limit use of external devices to those with an approved, documented business need. Monitor for use and attempted use of external devices. Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e., “thumb drives”), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares. Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted.

Control 8.4: Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables.

Control 8.5: Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature- based detection to identify and filter out malicious content before it arrives at the endpoint.

Control 8.6: Enable domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains.

Procedure 9: Limitation and Control of Network Ports, Protocols, and Services

Control 9.1: Ensure that only ports, protocols, and services with validated business needs are running on each system.

Control 9.2: Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

Control 9.3: Perform automated port scans on a regular basis against all key servers and compare to a known effective baseline. If a change that is not listed on the organization's approved baseline is discovered, an alert should be generated and reviewed.

Control 9.4: Verify any server that is visible from the Internet or an untrusted network, and if it is not required for business purposes, move it to an internal VLAN and give it a private address.

Control 9.5: Operate critical services on separate physical or logical host machines, such as DNS, file, mail, web, and database servers.

Control 9.6: Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized services or traffic should be blocked and an alert generated.

Procedure 10: Data Recovery Capability

Control 10.1: Ensure that each system is automatically backed up on at least a weekly basis, and more often for systems storing sensitive information. To help ensure the ability to rapidly restore a system from backup, the operating system, application software, and data on a machine should each be included in the overall backup procedure. These three components of a system do not have to be included in the same backup file or use the same backup software. There should be multiple backups over time, so that in the event of malware infection, restoration can be from a version that is believed to predate the original infection. All backup policies should be compliant with any regulatory or official requirements.

Control 10.2: Test data on backup media on a regular basis by performing a data restoration process to ensure that the backup isproperly working.

Control 10.3: Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.

Control 10.4: Ensure that key systems have at least one backup destination that is not continuously addressable through operating system calls. This will mitigate the risk of attacks like CryptoLocker which seek to encrypt or damage data on all addressable data shares, including backup destinations.

Procedure 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Control 11.1: Compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organization. The security configuration of such devices should be documented, reviewed, and approved by an organization change control board. Any deviations from the standard configuration or updates to the standard configuration should be documented and approved in a change control system.

Control 11.2: All new configuration rules beyond a baseline-hardened configuration that allow traffic to flow through network security devices, such as firewalls and network-based IPS, should be documented and recorded in a configuration management system, with a specific business reason for each change, a specific individual's name responsible for that business need, and an expected duration of the need.

Control 11.3: Use automated tools to verify standard device configurations and detect changes. All alterations to such files should be logged and automatically reported to security personnel.

Control 11.4: Manage network devices using two-factor authentication and encrypted sessions.

Control 11.5: Install the latest stable version of any security-related updates on all network devices.

Control 11.6: Network engineers shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading email, composing documents, or surfing the Internet.

Control 11.7: Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

Procedure 12: Boundary Defense

Control 12.1: Deny communications with (or limit data flow to) known malicious IP addresses (black lists), or limit access only to trusted sites (whitelists). Tests can be periodically carried out by sending packets from bogon source IP addresses (non- routable or otherwise unused IP addresses) into the network to verify that they are not transmitted through network perimeters. Lists of bogon addresses are publicly available on the Internet from various sources, and indicate a series of IP addresses that should not be used for legitimate traffic traversing the Internet.

Control 12.2: On DMZ networks, configure monitoring systems (which may be built in to the IDS sensors or deployed as a separate technology) to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border. This traffic should be sent to a properly configured Security Information Event Management (SIEM) or log analytics system so that events can be correlated from all devices on the network.

Control 12.3: Deploy network-based IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic.

Control 12.4: Network-based IPS devices should be deployed to complement IDS by blocking known bad signatures or the behavior of potential attacks. As attacks become automated, methods such as IDS typically delay the amount of time it takes for someone to react to an attack. A properly configured network-based IPS can provide automation to block bad traffic. When evaluating network-based IPS products, include those using techniques other than signature-based detection (such as virtual machine or sandbox-based approaches) for consideration.

Control 12.5: Design and implement network perimeters so that all outgoing network traffic to the Internet must pass through at least one application layer filtering proxy server. The proxy should

support decrypting network traffic, logging individual TCP sessions, blocking specific URLs, domain names, and IP addresses to implement a black list, and applying whitelists of allowed sites that can be accessed through the proxy while blocking all other sites. Organizations should force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter.

Control 12.6: Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication.

Control 12.7: All enterprise devices remotely logging into the internal network should be managed by the enterprise, with remote control of their configuration, installed software, and patch levels. For third-party devices (e.g., subcontractors/vendors), publish minimum security standards for access to the enterprise network and perform a security scan before allowing access.

Control 12.8: Periodically scan for back-channel connections to the Internet that bypass the DMZ, including unauthorized VPN connections and dual-homed hosts connected to the enterprise network and to other networks via wireless, dial-up modems, or other mechanisms.

Control 12.9: Deploy NetFlow collection and analysis to DMZ network flows to detect anomalous activity.

Control 12.10: To help identify covert channels exfiltrating data through a firewall, configure the built-in firewall session tracking mechanisms included in many commercial firewalls to identify TCP sessions that last an unusually long time for the given organization and firewall device, alerting personnel about the source and destination addresses associated with these long sessions.

Procedure 13: Data Protection

Control 13.1: Perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls.

Control 13.2: Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.

Control 13.3: Deploy an automated tool on network perimeters that monitors for sensitive information (e.g., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel.

Control 13.4: Conduct periodic scans of server machines using automated tools to determine whether sensitive data (e.g., personally identifiable information, health, credit card, or classified information) is present on the system in clear text. These tools, which search for patterns that indicate the presence of sensitive information, can help identify if a business or technical process is leaving behind or otherwise leaking sensitive information.

Control 13.5: If there is no business need for supporting such devices, configure systems so that they will not write data to USB tokens or USB hard drives. If such devices are required, enterprise software should be used that can configure systems to allow only specific USB devices (based on serial number or other unique property) to be accessed, and that can automatically encrypt all data placed on such devices. An inventory of all authorized devices must be maintained.

Control 13.6: Use network-based DLP solutions to monitor and control the flow of data within the network. Any anomalies that exceed the normal traffic patterns should be noted and appropriate action taken to address them.

Control 13.7: Monitor all traffic leaving the organization and detect any unauthorized use of encryption. Attackers often use an encrypted channel to bypass network security devices. Therefore, it is essential that organizations be able to detect rogue connections, terminate the connection, and remediate the infected system.

Control 13.8: Block access to known file transfer and email exfiltration websites.

Control 13.9: Use host-based data loss prevention (DLP) to enforce ACLs even when data is copied off a server. In most organizations, access to the data is controlled by ACLs that are implemented on the server. Once the data have been copied to a desktop system, the ACLs are no longer enforced and the users can send the data to whomever they want.

Procedure 14: Controlled Access Based on the Need to Know

Control 14.1: Segment the network based on the label or classification level of the information stored on the servers. Locate all sensitive information on separated VLANS with firewall filtering to ensure that only authorized individuals are only able to communicate with systems necessary to fulfill their specific responsibilities.

Control 14.2: All communication of sensitive information over less- trusted networks should be encrypted. Whenever information flows over a network with a lower trust level, the information should be encrypted.

Control 14.3: All network switches will enable Private Virtual Local Area Networks (VLANs) for segmented workstation networks to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attacker's ability to laterally move to compromise neighboring systems.

Control 14.4: All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

Control 14.5: Sensitive information stored on systems shall be encrypted at rest and require a secondary authentication mechanism, not integrated into the operating system, in order to access the information.

Control 14.6: Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data.

Control 14.7: Archived data sets or systems not regularly accessed by the organization shall be removed from the organization's network. These systems shall only be used as standalone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.

Procedure 15: Wireless Access Control

Control 15.1: Ensure that each wireless device connected to the network matches an authorized configuration and security profile, with a documented owner of the connection and a defined business need. Organizations should deny access to those wireless devices that do not have such a configuration and profile.

Control 15.2: Configure network vulnerability scanning tools to detect wireless access points connected to the wired network. Identified devices should be reconciled against a list of authorized wireless access points. Unauthorized (i.e., rogue) access points should be deactivated.

Control 15.3: Use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromises. In addition to WIDS, all wireless traffic should be monitored by WIDS as traffic passes into the wired network.

Control 15.4: Where a specific business need for wireless access has been identified, configure wireless access on client machines to allow access only to authorized wireless networks. For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration (basic input/output system or extensible firmware interface).

Control 15.5: Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection.

Control 15.6: Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which provide credential protectionand mutual authentication.

Control 15.7: Disable peer-to-peer wireless network capabilities on wireless clients.

Control 15.8: Disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need.

Control 15.9: Create separate virtual local area networks (VLANs) for BYOD systems or other untrusted devices. Internet access from this VLAN should go through at least the same border as corporate traffic. Enterprise access from this VLAN should be treated as untrusted and filtered and audited accordingly.

Procedure 16: Account Monitoring and Control

Control 16.1: Review all system accounts and disable any account that cannot be associated with a business process and owner.

Control 16.2: Ensure that all accounts have an expiration date that is monitored and enforced.

Control 16.3: Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails.

Control 16.4: Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

Control 16.5: Configure screen locks on systems to limit access to unattended workstations.

Control 16.6: Monitor account usage to determine dormant accounts, notifying the user or user's manager. Disable such accounts if not needed, or document and monitor exceptions (e.g., vendor

Maintenance accounts needed for system recovery or continuity operations). Require that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators should then disable accounts that are not assigned to valid workforce members.

Control 16.7: Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.

Control 16.8: Monitor attempts to access deactivated accounts through audit logging.

Control 16.9: Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

Control 16.10: Profile each user's typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works.

Control 16.11: Require multi-factor authentication for all user accounts that have access to sensitive data or systems. Multi-factor authentication can be achieved using smart cards, certificates, One Time Password (OTP) tokens, or biometrics.

Control 16.12: Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

Control 16.13: Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

Control 16.14: Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

Procedure 17: Security Skills Assessment and Appropriate Training to Fill Gaps

Control 17.1: Perform gap analysis to see which skills employees need to implement the other Controls, and which behaviors employees are not adhering to, using this information to build a baseline training and awareness roadmap for all employees.

Control 17.2: Deliver training to fill the skills gap. If possible, use more senior staff to deliver the training. A second option is to have outside teachers provide training onsite so the examples used will be directly relevant. If you have small numbers of people to train, use training conferences or online training to fill the gaps.

Control 17.3: Implement a security awareness program that (1) focuses on the methods commonly used in intrusions that can be blocked through individual action, (2) is delivered in short online modules convenient for employees (3) is updated frequently (at least annually) to represent the latest attack techniques, (4) is mandated for completion by all employees at least annually, (5) is reliably monitored for employee completion, and 6) includes the senior leadership team's personal messaging, involvement in training, and accountability through performance metrics.

Control 17.4: Validate and improve awareness levels through periodic tests to see whether employees will click on a link from suspicious email or provide sensitive information on the telephone without following appropriate procedures for authenticating a caller; targeted training should be provided to those who fall victim to the exercise.

Control 17.5: Use security skills assessments for each of the mission- critical roles to identify skills gaps. Use hands-on, real-world examples to measure mastery. If you do not have such assessments, use one of the available online competitions that simulate real-world scenarios for each of the identified jobs in order to measure mastery of skills mastery.

Procedure 18: Application Software Security

Control 18.1: For all acquired application software, check that the version you are using is still supported by the vendor. If not, update to the most current version and install all relevant patches and vendor security recommendations.

Control 18.2: Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks, including but not limited to cross-site scripting, SQL injection, command injection, and directory traversal attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host- based web application firewall should be deployed.

Control 18.3: For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.

Control 18.4: Test in-house-developed and third-party-procured web applications for common security weaknesses using automated remote web application scanners prior to deployment, whenever updates are made to the application, and on a regular recurring basis. In particular, input validation and output encoding routines of application software should be reviewed and tested.

Control 18.5: Do not display system error messages to end-users (output sanitization).

Control 18.6: Maintain separate environments for production and nonproduction systems. Developers should not typically have unmonitored access to production environments.

Control 18.7: For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.

Control 18.8: Ensure that all software development personnel receive training in writing secure code for their specific development environment.

Control 18.9: For in-house developed applications, ensure that development artifacts (sample data and scripts; unused libraries, components, debug code; or tools) are not included in the deployed software, or accessible in the production environment.

Procedure 19: Incident Response Management

Control 19.1: Ensure that there are written incident response procedures that include a definition of personnel roles for handling incidents. The procedures should define the phases of incident handling.

Control 19.2: Assign job titles and duties for handling computer and network incidents to specific individuals.

Control 19.3: Define management personnel who will support the incident handling process by acting in key decision-making roles.

Control 19.4: Devise organization-wide standards for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification. This reporting should also include notifying the appropriate Community Emergency Response Team in accordance with all legal or regulatory requirements for involving that organization in computer incidents.

Control 19.5: Assemble and maintain information on third-party contact information to be used to report a security incident (e.g., maintain an email address of security@company.com or have a web page http://company.com/security).

Control 19.6: Publish information for all personnel, including employees and contractors, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.

Control 19.7: Conduct periodic incident scenario sessions for personnel associated with the incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling team.

Procedure 20: Penetration Tests and Red Team Exercises

Control 20.1: Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. Penetration testing should occur from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization) as well as from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks.

Control 20.2: Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.

Control 20.3: Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.

Control 20.4: Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, emails or documents containing passwords or other information critical to system operation.

Control 20.5: Plan clear goals of the penetration test itself with blended attacks in mind, identifying the goal machine or target asset. Many APT-style attacks deploy multiple vectors— often social engineering combined with web or network exploitation. Red Team manual or automated testing that captures pivoted and multi-vector attacks offers a more realistic assessment of security posture and risk to critical assets.

Control 20.6: Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.

Control 20.7: Wherever possible, ensure that Red Teams results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.

Control 20.8: Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.