Bad Dinosaur

Digital Infrastructure and Data Security Policy

Updated: 9th of August 2019 - Russ Peterson

1. **Policy Statement**
    a. The purpose of this document is to provide a security framework that will ensure the protection of all hosted infrastructure and its data. Failure to comply with this security policy may subject you to disciplinary action.
2. **Who is affected by this policy**
    a. All employees and subcontractors of Bad Dinosaur working with digital infrastructure.
3. **Definitions**
    a. Digital Infrastructure
        i. Any computer, server, storage device or service whether remote or otherwise that holds digital data.
    b. Data
        i. Information processed or stored by a computer. This information may be in the form of text documents, images, audio clips, software programs, or other types of data generated or owned by Bad Dinosaur or any of its clients.
    c. Authorization
        i. The function of establishing an individual's privilege levels to access and/or handle information.
    d. Availability
        i. Ensuring that information is ready and suitable for use.
    e. Confidentiality
        i. Ensuring that information is kept in strict privacy.
    f. Integrity
        i. Ensuring the accuracy, completeness, and consistency of information.
    g. Unauthorized access
        i. Looking up, reviewing, copying, modifying, deleting, analyzing, or handling information without proper authorization and legitimate business need
4. **Confidentiality classification**
    a. All data and information relating to data stored on digital infrastructure
5. **Responsibilities**
    a. All employees and subcontractors of Bad Dinosaur working with digital infrastructure are expected to:
        i. Fully comply with the Bad Dinosaur Information Security Policy.
        ii. Fully comply with the "Every Employee Security Checklist".

iii. Fully comply with any policies implemented by the client.
iv. Access data and information only as needed to meet legitimate business needs.
v. Protect the confidentiality, integrity and availability of information in a manner consistent with this security policy and any such policies provided by the client.
vi. Safeguard any access details (such as username and password) that allows one to access data hosted on digital infrastructure.
vii. Safeguard “publishing profiles” that allows one to publish applications to digital infrastructure.
viii. Safeguard “connection strings” that allows one to access data on remote databases.
ix. Ensure that any infrastructure created at a remote location is accessible only by the Bad Dinosaur office IP address or any other IP address authorised by the directors or security officers of Bad Dinosaur.
x. Ensure all data transferred between physical locations is transferred securely using encryption.
xi. Ensure all data stored in any location is stored securely using encryption.
xii. Immediately report any known breach, weakness or concerns to the directors or security officers of Bad Dinosaur.
xiii. Contact the directors of Bad Dinosaur prior to disclosing information generated by that Office or prior to responding to any litigation or law enforcement subpoenas,court orders, and other information requests from private litigants and government agencies.
xiv. Contact the directors of Bad Dinosaur prior to responding to requests for information from regulatory agencies, inspectors, examiners, and/or auditors.

6. Related procedures and Policies

a. Bad Dinosaur Information Security Policy
b. Every Employee Security Checklist

7. Review

a. At a minimum, this policy shall be reviewed by the directors or security officers of Bad Dinosaur every 12 months.