**Information Security Policy: Backup Policy**

**Policy Statement:**

This Backup Policy outlines the procedures and requirements for the regular and secure backup of company data. The goal is to ensure the availability and recoverability of critical information in the event of data loss, system failures, or other unforeseen incidents.

**1. Data Backup Requirements:**

a. **Regular Schedule:** All critical company data must be regularly backed up according to the schedule defined by the IT department.

b. **Data Types:** Backups should include, but not be limited to, databases, documents, configurations, and any other data deemed essential for business continuity.

c. **Offsite Storage:** Backup copies must be stored in a secure offsite location to mitigate the risk of data loss in the event of on-site disasters.

**2. Backup Verification:**

a. **Periodic Testing:** Regular testing of backup restoration procedures should be conducted to ensure the reliability of the backup system.

b. **Verification Logs:** Maintain logs that document backup activities, including successful completions and any issues encountered.

**3. Waiver for Non-Backup:**

a. **Waiver Option:** In situations where a business unit or individual does not wish to have their data backed up, they must formally express this preference to the IT department.

b. **Waiver Form:** Individuals opting out of data backup must sign a waiver acknowledging that they understand the risks associated with data loss and release the company from any responsibility for the recovery of their lost data.

c. **Exception Review:** The IT department will review waiver requests to ensure they align with business needs and do not compromise the overall security and continuity of company operations.

**4. Responsibilities:**

a. **IT Department:** The IT department is responsible for implementing and maintaining the backup systems, defining backup schedules, and ensuring the successful completion of backup tasks.

b. **Users:** Users are responsible for identifying critical data, reporting any discrepancies in the backup process, and promptly notifying the IT department of any data loss incidents.

**5. Data Restoration:**

a. **Authorized Request:** Data restoration requests must be submitted through authorized channels, and only authorized personnel may initiate the restoration process.

b. **Priority Restoration:** Critical data required for business operations will be given priority during the restoration process.

**6. Policy Review:**

This policy will be subject to periodic review and updates to align with industry best practices and emerging cybersecurity threats.

**Acknowledgment:**

By using company systems and services, users acknowledge their understanding of and commitment to complying with this Backup Policy.

*Date of Policy Implementation: (DATE)*

*Policy Owner: (COMPANY NAME)*