Be Ready Utah

✓ Make a Plan
✓ Get a Kit
✓ Be Informed
✓ Get Involved

Business Security Assessment Tool

The attached Assessment Tool is designed to help you assess your organization’s strengths and weaknesses with respect to security issues. Please use this tool to evaluate each area, which will provide an assessment of where your office stands today. You will find helpful information and suggestions that will assist you in each area. **Remember every action you take will positively impact your organization’s mission.**

Rating Scale

1	**=**	**Fully Implemented**
2	**=**	**Implementation Planned**
3	**=**	**Non-Existent**

## Written Policies and Procedures	**1**	**2**	**3**
1. The agency has a security mission statement.	○	○	○
2. There is a formal definition of objectives and formal policy statement on security endorsed by agency management.	○	○	○
3. There is a formal manual defining the agency’s security standards and procedures.	○	○	○
4. Changes in security practices are incorporated into the manual and disseminated to staff.	○	○	○
TOTAL =	□	□	□

Scoring: Written Policies and Procedures

Total this section adding the value from each column (1=1, 2=2, 3=3)

If you scored:

4-6	=	No action necessary.
7-12	=	Review written policies and procedures.

Rating Scale

1	**=**	**Fully Implemented**
2	**=**	**Implementation Planned**
3	**=**	**Non-Existent**

Physical Security

	1	**2**	**3**
1. Employees are required to wear ID badges.	○	○	○
2. Access to the building is controlled.	○	○	○
3. Armed security guards are present.	○	○	○
4. Procedures are established concerning possession of weapons; visitors are either permitted to possess weapons, or are disarmed. If visitors are disarmed, there is a secured holding place for the weapon.	○	○	○
5. Interview rooms or offices where the public is present with a worker are supplied with panic buttons. Polices and procedures are in place for action when the button is activated.	○	○	○
6. Interview rooms are separate from employee work areas.	○	○	○
7. Video cameras are placed in strategic locations throughout the office.	○	○	○
8. All public access entryways have metal detectors.	○	○	○
9. All employee parking areas are sufficiently lighted.	○	○	○
10. Cypher lock codes are frequently changed.	○	○	○
11. Furniture in interview rooms is situated for employees to have direct and easy exit (escape route).	○	○	○
12. Reception personnel are protected with bulletproof glass.	○	○	○
13. The public utilizes separate bathrooms.	○	○	○
14. Procedures are in place that dictate appropriate responses to viral and bacterial threats (Anthrax, etc.).	○	○	○
15. Procedures are in place that dictate appropriate security and safety drills.	○	○	○
16. State or local police departments provide periodic security assessments.	○	○	○
17. Contact numbers for police, fire, and emergency personnel are easily accessible to all staff.	○	○	○
TOTAL =	□	□	□

Scoring: Physical Security

Total this section adding the value from each column (1=1, 2=2, 3=3)

If you scored:

17-20	=	No action necessary.
21-51	=	The safety of your staff and information may be at risk. Review the physical security section and carefully evaluate any answers that are marked 2 or 3.

Rating Scale

1	**=**	**Fully Implemented**
2	**=**	**Implementation Planned**
3	**=**	**Non-Existent**

Personnel

	1	**2**	**3**
1. Job descriptions include accountability for security.	○	○	○
2. Applicant references and backgrounds are fully checked prior to employment.	○	○	○
3. Security and reference checks are completed on temporary and contract staff.	○	○	○
4. All employees sign a non-disclosure statement (or equivalent) at hire and annually.	○	○	○
5. Management personnel are responsible for security awareness on the part of the staff.	○	○	○
6. Management has taken steps to ensure that ALL employees are aware of the security polices and procedures.	○	○	○
7. Continuous updating of policies and procedures has been arranged to ensure that new or revised requirements are accommodated.	○	○	○
8. Policies, procedures, and disciplinary actions have been established to deal with misuse of data.	○	○	○
9. There are written policies on conflicts of interest, outside employment, accepting gifts, drug and alcohol abuse, and stealing company property.	○	○	○
10. There are written policies that address falsifying records.	○	○	○
11. Security responsibilities are included in employees' performance evaluations.	○	○	○
12. Personnel are penalized for security violations.	○	○	○
TOTAL =	□	□	□

Scoring: Personnel

Total this section adding the value from each column (1=1, 2=2, 3=3)

If you scored:

12-14 = No action necessary.

15-36 = Your personnel practices may leave your agency open to negligence in hiring. Review the personnel section and carefully evaluate any answers that are marked 2 or 3.

Rating Scale

1 = Fully Implemented
2 = Implementation Planned
3 = Non-Existent

Training

	1	**2**	**3**
1. Employees are trained not to leave computer terminals unattended.	○	○	○
2. A security training plan has been developed.	○	○	○
3. Training programs include a review of security objectives and polices.	○	○	○
4. Security training is delivered to all staff regularly and consistently per an established schedule.	○	○	○
5. Employees are trained on proper disposal of confidential documents to include secure containers and shredding of data.	○	○	○
6. All employees are trained in their roles and responsibilities as outlined in emergency, disaster response, and contingency plans.	○	○	○
7. Management is involved in measuring the effectiveness of the security initiatives.	○	○	○
8. Staff has been assigned, trained, and participated in tests of emergency, disaster response, and contingency plans.	○	○	○
TOTAL =	□	□	□

Scoring: Training

Total this section adding the value from each column (1=1, 2=2, 3=3)

If you scored:

8-11 = No action necessary.

12-24 = Your training practices may need to be reviewed to provide increased safety in the workplace. Review the training section and carefully evaluate any answers that are marked 2 or 3.

Rating Scale

1	**=**	**Fully Implemented**
2	**=**	**Implementation Planned**
3	**=**	**Non-Existent**

Budget/Resources

	1	**2**	**3**
1. Budget and resources are dedicated to security initiatives.	○	○	○
2. Budget and resources are actually spent on security initiatives.	○	○	○
3. There a dedicated full-time Information System Security Officer (ISSO).	○	○	○
TOTAL =	□	□	□

Scoring: Budget/Resources

Total this section adding the value from each column (1=1, 2=2, 3=3)

If you scored:

3	=	No action necessary.
4-9	=	Your budget and resources may need to be reviewed to ensure security is a priority. Review the budget and resource section and carefully evaluate any answers that are marked 2 or 3.

Rating Scale

1	**=**	**Fully Implemented**
2	**=**	**Implementation Planned**
3	**=**	**Non-Existent**

Technical

	1	**2**	**3**
1. Employees follow strict password and log-on protection procedures.	○	○	○
2. Virus detection and elimination software is installed on each personal computer.	○	○	○
3. Virus detection and elimination software is regularly updated automatically or manually.	○	○	○
4. Audit trails are established and monitored to prevent/reduce misuse of data.	○	○	○
5. PCs are monitored closely to prohibit the installation of off-the-shelf and pirated software.	○	○	○
6. User access is restricted to minimum necessary to perform the job.	○	○	○
7. System tests are regularly conducted to determine if it is “hacker” proof.	○	○	○
8. All connections go through a “firewall” system.	○	○	○

Technical

	1	2	3
9. Transmission of sensitive data is protected from unauthorized disclosure through encryption.	○	○	○
TOTAL =	□	□	□

Scoring: Technical

Total this section adding the value from each column (1=1, 2=2, 3=3)

If you scored:

9-11 = No action necessary.

12-27 = Your technical resources may need to be reviewed to tighten security. Review the technical section and carefully evaluate any answers that are marked 2 or 3.

Rating Scale

1 = Fully Implemented
2 = Implementation Planned
3 = Non-Existent

Contingency Plans

	1	2	3
1. Contingency plans are in place in the event of loss of personnel (strike, etc.), disasters, and emergencies.	○	○	○
2. Contingency plans specify who will (and how to) notify customers and staff in the event that the office is inoperable.	○	○	○
3. Contingency plans assign individual and team responsibilities in order to expedite mobilization of personnel.	○	○	○
4. Contingency plans are available that address back-up and recovery procedures.	○	○	○
5. Contingency plans have been tested and measured for effectiveness.	○	○	○
TOTAL =	□	□	□

Scoring: Contingency Plans

Total this section adding the value from each column (1=1, 2=2, 3=3)

If you scored:

5-7 = No action necessary.

7-15 = Your contingency plans may need to be reviewed to ensure ongoing operations. Review the Contingency Plans section and carefully evaluate any answers that are marked 2 or 3.